Deutscher Bundestag
11. Wahlperiode

Drucksache 11/8200

24. 10. 90

Sachgebiet 204

Beschlußempfehlung und Bericht

des Innenausschusses (4. Ausschuß)

zu den Unterrichtungen durch den Bundesbeauftragten für den Datenschutz

a) Achter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)
— Drucksache 10/4690 —

b) Neunter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)
— Drucksache 10/6816 —

A. Problem

Gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes hat der Bundesbeauftragte für den Datenschutz beginnend mit dem 1. Januar 1979 einen jährlichen Tätigkeitsbericht zu erstellen.

B. Lösung

Im Achten und Neunten Tätigkeitsbericht informiert der Bundesbeauftragte für den Datenschutz detailliert und umfassend über seine Tätigkeit in den Jahren 1985 und 1986, über seine Rechtsauffassungen, Beanstandungen, Anregungen und Forderungen zu datenschutzrechtlichen Fragen.

Die Beschlußempfehlung des Innenausschusses enthält als Stellungnahme zu diesen Berichten Feststellungen und Empfehlungen, insbesondere zu Themen aus dem Bereich der Deutschen Bundespost, des Arbeitnehmer/innen-Datenschutzes, des Personalaktenrechts, des Wehrpflichtgesetzes, des Bundesamtes für Verfassungsschutz und des Bundeskriminalamtes. Im Laufe der Beratungen wurden hinsichtlich vieler diskutierter Fragen, insbesondere aus dem Bereich des Bundesamtes für Verfassungsschutz und dem Bereich des Bundeskriminalamtes, Lösungen erarbeitet,

die die mehrheitliche Zustimmung des Ausschusses fanden. Auf eine Aufnahme der betreffenden Themen in die Beschlußempfehlung konnte daher verzichtet werden.

Mehrheitsentscheidung im Ausschuß gegen die Stimmen der Fraktion der SPD und der Fraktion DIE GRÜNEN

C. Alternativen

Die Fraktion der SPD hat einen eigenen Vorschlag für eine Beschlußempfehlung vorgelegt, der ebenfalls datenschutzrechtliche Probleme aus den Bereichen der Deutschen Bundespost, des Personalwesens, des Bundesamtes für Verfassungsschutz und des Bundeskriminalamtes aufgreift. Die Vorschläge der Fraktion der SPD stimmen insoweit in mehreren Punkten mit der mehrheitlich gefaßten Beschlußempfehlung überein, so z. B. hinsichtlich der Anregung einer strikten Trennung von Beihilfestellen und Personalstellen, hinsichtlich des Vorschlags der Kennzeichnung zu löschender Daten in Unterlagen des Bundeskriminalamtes, die sowohl zu löschende als auch weiterhin zu speichernde Daten enthalten, durch Stempelaufdruck und hinsichtlich der Anregung, eine dreijährige Wiedervorlagefrist für in APIS gespeicherte Daten einzuführen. Darüber hinaus sind in dem Alternativvorschlag der Fraktion der SPD Aufforderungen zu den Themenbereichen „Ablaufen des Übergangsbonus", „Stellenforderungen des Bundesbeauftragten für den Datenschutz", „Rechtswesen", „Besoldung und Versorgung", „Zusatzerhebungen bei Kfz-Anmeldungen durch Ausländer", „Neufassung der Sicherheitsüberprüfungsrichtlinien" und „Datensicherung beim Einsatz von Personalcomputern" enthalten.

Die Fraktion DIE GRÜNEN hat einen Alternativvorschlag für eine Beschlußempfehlung vorgelegt, in dem sie sich aus ihrer Sicht ebenfalls zu datenschutzrechtlichen Fragen aus den Bereichen der Deutschen Bundespost, der automatisierten Personaldatenverarbeitung, des Wehrpflichtgesetzes, des Bundesamtes für Verfassungsschutz und des Bundeskriminalamtes äußert. Darüber hinaus enthält ihr Vorschlag Empfehlungen hinsichtlich einer Löschung des Ausländerzentralregisters, hinsichtlich eines Verbotes von Videoaufzeichnungen auf Bahnhöfen sowie hinsichtlich einer eingeschränkten Datenübermittlung an das Ausland.

D. Kosten

Keine

Beschlußempfehlung

Der Bundestag wolle beschließen:

1. Der Deutschen Bundespost wird empfohlen, bei der Genehmigung von Satellitenfunkempfangsanlagen personenbezogene Daten im Wege der Amtshilfe nur in dem nach Landesrecht unabdingbar erforderlichen Umfang an die rundfunkrechtlich zuständigen Landesanstalten weiterzugeben.

   Es wird begrüßt, daß die Deutsche Bundespost aufgrund der Anregungen des Bundesbeauftragten für den Datenschutz das Verfahren der Weitergabe der Anschriften zu Werbezwecken an die Deutsche Postreklame GmbH zugunsten der Fernsprechteilnehmer besser und sicherer ausgestaltet hat. Die Deutsche Bundespost sollte allerdings noch einmal prüfen, ob die Eintragungspflicht des Teilnehmers in das Telefonbuch nicht etwas weniger restriktiv gehandhabt werden könnte. Schließlich wird es begrüßt, daß die Deutsche Bundespost die Praxis der Anschriftenermittlung durch die Zusteller für eine gezielte Werbung für den Postsparkassendienst überprüft.

2. Der Bundesregierung wird empfohlen, noch in dieser Legislaturperiode einen Gesetzentwurf zu einer bereichsspezifischen Regelung des Arbeitnehmer/innen-Datenschutzes sowie des Personalaktenrechts so rechtzeitig vorzulegen, daß er noch in dieser Legislaturperiode abschließend beraten werden kann.

   Die Bundesregierung wird aufgefordert, auch schon vor Inkrafttreten eines neuen Personalaktenrechts in allen Teilen der Bundesverwaltung eine Trennung von Beihilfestellen und Personalstellen herbeizuführen. Mit der Automatisierung im Bereich des Beihilfewesens soll erst begonnen werden, wenn diese Trennung vorgenommen worden ist.

3. Es ist sicherzustellen, daß die beabsichtigte Zusammenlegung der Eignungs- und Verwendungsprüfung mit der Musterung nach § 20a Wehrpflichtgesetz nicht dazu führt, daß ein Wehrpflichtiger, der erst während des Musterungsverfahrens einen Antrag auf Kriegsdienstverweigerung stellt, neben der Musterung auch noch dieser besonderen Prüfung unterzogen wird.

4. Die Weitergabe von Daten durch das Bundesamt für Verfassungsschutz soll in den in dieser Wahlperiode zu verabschiedenden einschlägigen Gesetzen ausdrücklich geregelt werden.

5. Die Bundesregierung wird aufgefordert sicherzustellen, daß das Bundeskriminalamt zu löschende Daten nach Ziffer 8.1 der Dateirichtlinien durch Stempelaufdruck kenntlich macht.

6. Die Bundesregierung wird gebeten, das von ihr praktizierte Verfahren hinsichtlich des Zugriffs auf die Falldatei Rauschgift des Bundeskriminalamtes beizubehalten.

7. Es wird festgestellt, daß das Problem der Aufnahme dritter Personen in die Dateien des Bundeskriminalamtes einer ausdrücklichen Regelung in den in Frage kommenden zu erlassenden Gesetzen bedarf.

8. Es wird festgestellt, daß für gemeinsame Dateien des Bundeskriminalamtes und anderer Polizeibehörden in zukünftigen Gesetzen folgende Regelung sinnvoll ist:

   Die Verantwortung einer speichernden Stelle im Sinne der allgemeinen Vorschriften des Datenschutzrechtes trägt jede Stelle, die Daten eingestellt hat, für die von ihr eingegebenen Daten; nur sie darf diese Daten verändern, sperren oder löschen. Die eingebende Stelle muß feststellbar sein.

9. Die Bundesregierung wird aufgefordert, für alle in APIS gespeicherten Datensätze eine Wiedervorlagefrist von 3 Jahren einzuführen.

10. Es wird festgestellt, daß die Voraussetzungen für die Anlage von SPUDOK-Dateien in dem zu erlassenden Bundeskriminalamtgesetz bzw. in der Strafprozeßordnung zu regeln sind.

Bonn, den 11. September 1989

Der Innenausschuß

Bernrath	**Dr. Blens**	**Dr. Hirsch**	**Wartenberg (Berlin)**	**Frau Dr. Vollmer**
Vorsitzender	Berichterstatter			

Bericht der Abgeordneten Dr. Blens, Dr. Hirsch, Wartenberg (Berlin) und Frau Dr. Vollmer

I. Allgemeines

Der Achte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz — Drucksache 10/4690 — wurde in der 255. Sitzung des Deutschen Bundestages am 10. Dezember 1986 und der Neunte Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz — Drucksache 10/6816 — in der 30. Sitzung des Deutschen Bundestages am 8. Oktober 1987 an den Innenausschuß federführend sowie an den Rechtsausschuß, den Ausschuß für Wirtschaft, den Ausschuß für Arbeit und Sozialordnung, den Verteidigungsausschuß, den Ausschuß für das Post- und Fernmeldewesen sowie den Ausschuß für Forschung und Technologie zur Mitberatung überwiesen. Darüber hinaus wurde der Achte Tätigkeitsbericht an den Ausschuß für Jugend, Familie, Frauen und Gesundheit und der Neunte Tätigkeitsbericht an den Ausschuß für Raumordnung, Bauwesen und Städtebau überwiesen. Der Ausschuß für Jugend, Familie, Frauen und Gesundheit hat entsprechend seiner in seiner Sitzung am 9. März 1988 geäußerten Absicht gutachtlich zum Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz Stellung genommen. Hinsichtlich des Achten Tätigkeitsberichts erfolgte eine erneute Überweisung mit Drucksache 11/883 vom 2. Oktober 1987, Nummer 27 in der 30. Sitzung des Deutschen Bundestages am 8. Oktober 1987.

Der Innenausschuß hat den Achten und den Neunten Tätigkeitsbericht in seiner 12. Sitzung am 14. Oktober 1987 anberaten. Eine Fortsetzung der Ausschußberatungen erfolgte in der 37. Sitzung am 23. November 1988, der 40. Sitzung am 7. Dezember 1988, der 42. Sitzung am 25. Januar 1989 und der 43. Sitzung am 15. Februar 1989. In seiner 51. Sitzung am 26. April 1989 hat er mit den Stimmen der Koalitionsfraktionen gegen die Stimmen der Fraktion der SPD und der Fraktion DIE GRÜNEN die o. g. Beschlußempfehlung angenommen. Der Vorschlag der Fraktion der SPD für eine Beschlußempfehlung wurde mit den Stimmen der Koalitionsfraktionen gegen die Stimmen der Fraktion der SPD bei Enthaltung der Fraktion DIE GRÜNEN abgelehnt. Die Alternativvorschläge der Fraktion DIE GRÜNEN für die Ausgestaltung der Beschlußempfehlung wurden mit den Stimmen der Koalitionsfraktionen gegen die Stimmen der Fraktion DIE GRÜNEN bei Enthaltung der Fraktion der SPD abgelehnt. Darüber hinaus sind insbesondere die Bereiche des Bundesamtes für Verfassungsschutz, des Bundeskriminalamtes und des Bundesnachrichtendienstes in zehn intensiven Berichterstattergesprächen erörtert worden. Diese fanden im Zeitraum vom 11. November 1987 bis zum 10. November 1988 unter Beteiligung weiterer Mitglieder des Ausschusses, der Bundesregierung sowie des Bundesbeauftragten für den Datenschutz statt.

II. Empfehlungen der mitberatenden Ausschüsse

1. Der Rechtsausschuß hat mit Mehrheit dem Antrag der Fraktionen der CDU/CSU und der FDP zugestimmt, den Achten und Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis zu nehmen.

   Mit Mehrheit abgelehnt worden war folgender Antrag der Fraktion der SPD:

   „Der Rechtsausschuß nimmt die Berichte des Datenschutzbeauftragten zustimmend zur Kenntnis.

   Der Rechtsausschuß stellt fest, daß die Vorschläge und Beanstandungen immer noch nicht umgesetzt sind und fordert die Bundesregierung auf, unverzüglich tätig zu werden.

   Insbesondere sind die Vorlagen für das Justizmitteilungsgesetz, das Bundeszentralregistergesetz und die Vorschriften über das Schuldnerverzeichnis bis zum 1. September 1988 vorzulegen. Die weiteren bereichsspezifischen Datenschutzvorschriften sollen bis spätestens ein Jahr vor Ablauf der Wahlperiode vorgelegt sein."

   Ebenfalls mit Mehrheit abgelehnt worden waren zahlreiche Anträge der Fraktion DIE GRÜNEN.

2. Der Ausschuß für Wirtschaft hat beide Tätigkeitsberichte bei drei Gegenstimmen von Mitgliedern der Fraktion DIE GRÜNEN zur Kenntnis genommen.

3. Der Ausschuß für Arbeit und Sozialordnung hat den Achten und Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zur Kenntnis genommen und dem Bundesbeauftragten und seinen Mitarbeitern für die geleistete Arbeit gedankt.

   Der Ausschuß hat die Auffassung vertreten, daß bei allen Sozialversicherungsträgern im Rahmen einer Tätigkeit in den Selbstverwaltungsorganen und besonderen Ausschüssen (§ 36a SGB IV) weder dem Arbeitgeber selbst noch einem anderen Vorgesetzten noch einem Angehörigen der Personalverwaltung Kenntnisse von personenbezogenen Daten eines Betriebsangehörigen offenbart werden dürften, die dem Sozialgeheimnis unterlägen. Die Bundesregierung werde daher um Prüfung gebeten, wie sichergestellt werden könne, daß diese Personen bei der Einsichtnahme in Daten von Betriebsangehörigen, die dem Sozialgeheimnis unterlägen, und bei deren Erörterung nicht mitwirkten und durch andere Personen vertreten würden.

   Darüber hinaus solle sichergestellt werden, daß der Arbeitgeber nicht Personen zur Führung der Ge-

schäfte der Betriebskrankenkasse bestelle, die befugt seien, gleichzeitig Aufgaben im Personalbereich des Betriebes oder Dienstbetriebes wahrzunehmen.

Der Ausschuß für Arbeit und Sozialordnung hat der Bundesregierung empfohlen, noch in dieser Legislaturperiode einen Gesetzentwurf zu einer bereichsspezifischen Regelung des Arbeitnehmer/innen-Datenschutzes sowie des Personalaktenrechts so rechtzeitig vorzulegen, daß er noch in dieser Legislaturperiode abschließend beraten werden könne.

4. Der Verteidigungsausschuß hat die seine Zuständigkeit betreffenden Bereiche des Achten und Neunten Tätigkeitsberichtes des Bundesbeauftragten für den Datenschutz erörtert und die Berichte mit den Stimmen der Fraktion der CDU/CSU, SPD und FDP bei Enthaltung der Fraktion DIE GRÜNEN zur Kenntnis genommen.

5. Der Ausschuß für das Post- und Fernmeldewesen hat den Achten und Neunten Bericht des Bundesbeauftragten für den Datenschutz mit Interesse zur Kenntnis genommen. Der Ausschuß hat die Straffung und die Unterscheidung zwischen Rechtsverstößen und Anregungen begrüßt. Er hat empfohlen, Einzelfälle nur in gravierenden Fällen in den Bericht aufzunehmen, wenn sie grundsätzliche Tendenzen für die Sicherung und Fortentwicklung des Datenschutzes erkennen ließen. Der Ausschuß erwartet, daß die Deutsche Bundespost ihre Bemühungen um eine Verbesserung der Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz fortsetzt und ihn über datenschutzrechtlich wesentliche Vorgänge möglichst frühzeitig und zügig informiert.

   Der Deutschen Bundespost wurde empfohlen, bei der Genehmigung von Satellitenfunkempfangsanlagen personenbezogene Daten im Wege der Amtshilfe nur in dem nach Landesrecht unabdingbar erforderlichen Umfang an die rundfunkrechtlich zuständigen Landesanstalten weiterzugeben.

   Der Ausschuß hat begrüßt, daß die Deutsche Bundespost aufgrund der Anregungen des Bundesbeauftragten für den Datenschutz das Verfahren der Weitergabe der Anschriften zu Werbezwecken an die Deutsche Postreklame GmbH zugunsten der Fernsprechteilnehmer besser und sicherer ausgestaltet habe. Die Deutsche Bundespost solle allerdings noch einmal prüfen, ob die Eintragungspflicht des Teilnehmers in das Telefonbuch nicht etwas weniger restriktiv gehandhabt werden könne. Der Ausschuß begrüßte letztlich, daß die Deutsche Bundespost die Praxis der Anschriftenermittlung durch die Zusteller für eine gezielte Werbung für den Postsparkassendienst überprüfe.

   Der Ausschuß hat den Innenausschuß gebeten, die Frage zu klären, ob der Bundesbeauftragte für den Datenschutz das Recht habe, mit den Personalvertretungen bei den Behörden unmittelbar Verbindung aufzunehmen, oder ob die in der Stellungnahme der Bundesregierung zum Neunten Tätigkeitsbericht von der Deutschen Bundespost vertretene Auffassung

   „Die Deutsche Bundespost legt Wert darauf, daß der Bundesbeauftragte für den Datenschutz sich nur an die im Bundesdatenschutzgesetz als Normadressaten genannten Behörden und sonstigen öffentlichen Stellen wendet. Dies schließt einen direkten Zugang des Bundesbeauftragten für den Datenschutz zu den Personalvertretungen bei den Behörden aus, da Personalvertretungen keine selbständigen Behörden oder sonstigen öffentlichen Stellen sind."

   zutreffe.

6. Der Ausschuß für Forschung und Technologie hat beide Tätigkeitsberichte einvernehmlich zur Kenntnis genommen.

7. Der Ausschuß für Jugend, Familie, Frauen und Gesundheit hat den Achten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz einstimmig zur Kenntnis genommen und zum Neunten Tätigkeitsbericht eine gutachtliche Stellungnahme abgegeben. Danach hat der Ausschuß für Jugend, Familie, Frauen und Gesundheit auch den Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz einstimmig zustimmend zur Kenntnis genommen.

   Nach Auffassung des Ausschusses muß jedoch sichergestellt werden, daß die beabsichtigte Zusammenlegung der in Abschnitt 18 Punkt 3 des Berichts angesprochenen Eignungs- und Verwendungsprüfungen mit der Musterung nicht dazu führt, daß ein Wehrpflichtiger, der erst während des Musterungsverfahrens einen Antrag auf Kriegsdienstverweigerung stellt, neben der Musterung auch noch dieser besonderen Prüfung unterzogen wird.

8. Der Ausschuß für Raumordnung, Bauwesen und Städtebau hat den Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz beraten und sich dabei mit den Bemerkungen zu §§ 24 ff., § 138 und § 195 des Baugesetzbuchs befaßt. Er hat diesen Bericht zur Kenntnis genommen.

III. Die Beratungen im Innenausschuß

1. Beratungsmaterialien

Die Bundesregierung hat entsprechend dem Beschluß des Deutschen Bundestages zum Zweiten und Dritten Tätigkeitsbericht (vgl. Drucksache 9/1623) dem Innenausschuß ausführliche Stellungnahmen zum Achten und Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz zugeleitet, die auch den mitberatenden Ausschüssen im Rahmen ihrer Beratungen zur Verfügung gestanden haben. In diesen wird dargelegt, in welchem Umfang den Beanstandungen und Anregungen des Bundesbeauftragten für den Datenschutz bereits Rechnung getragen worden ist, Maßnahmen eingeleitet oder geplant sind, und in welchem Umfang die Bundesregierung gegenüber dem Bundesbeauftragten für den Datenschutz abwei-

chende Rechts- oder Sachauffassungen vertritt. Die Stellungnahmen der Bundesregierung sind diesem Bericht als Anlage beigefügt. Dadurch soll deutlich werden, warum es dem Ausschuß ausreichend erschien, nur zu den in diesem Bericht aufgegriffenen Einzelfragen Aussagen zu treffen. Der Innenausschuß hat in seinen Beratungen neben dem Achten und Neunten Tätigkeitsbericht zudem einen zusätzlichen Prüfbericht des Bundesbeauftragten für den Datenschutz über eine datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamtes einbezogen, die in der Zeit vom 1. Dezember 1987 bis zum 29. Januar 1988 durchgeführt worden war. Zudem lag dem Innenausschuß die Stellungnahme der Bundesregierung zu diesem zusätzlichen Prüfbericht vor. Sowohl dieser zusätzliche Prüfbericht als auch die Stellungnahme der Bundesregierung hierzu waren von der jeweils herausgebenden Stelle insgesamt als Verschlußsache — Nur für den Dienstgebrauch — gekennzeichnet worden. Der Innenausschuß hat des weiteren einen als vertraulich eingestuften, gesonderten Prüfbericht des Bundesbeauftragten für den Datenschutz — betreffend die Abteilung V des Bundesamtes für Verfassungsschutz — einbezogen, der vom 11. Dezember 1987 datiert.

2. Allgemeines zu der Beschlußempfehlung und zu den Beschlußempfehlungsvorschlägen der Oppositionsfraktionen

Seitens der Koalitionsfraktionen wurde die Ansicht vertreten, daß zwischen den Fraktionen mehr Übereinstimmung bestehe, als in der Beschlußempfehlung und den jeweiligen Entschließungsvorschlägen der Oppositionsfraktionen zum Ausdruck komme. Man habe sich bei der Abfassung der Entschließung der Koalitionsfraktionen auf das unbedingt Notwendige beschränkt. Es seien aus den Berichterstattergesprächen zahlreiche Punkte offengeblieben, auf die man bei den anstehenden Gesetzesberatungen zurückkommen müsse, so daß es wenig Sinn habe, sie vorab festzulegen. Man danke dem Bundesbeauftragten für seinen Bericht.

Auch seitens der Fraktion der SPD wurde dem Bundesbeauftragten für seinen Bericht gedankt. Die Fraktion der SPD hielt es für enttäuschend, daß mehrere Themen, die vor allem in den Berichterstattergesprächen ausführlich diskutiert worden seien, in der Beschlußempfehlung nicht angesprochen worden seien, so z. B. die Speicherung personengebundener Hinweise und Probleme im Zusammenhang mit Speicherungen in APIS und NADIS. Insbesondere habe der Inhalt des zusätzlichen Prüfberichts des Bundesbeauftragten für den Datenschutz über die Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamts keinen Eingang in die Beschlußempfehlung gefunden. Auch wenn es mehrere Punkte in der Beschlußempfehlung gebe, in denen Übereinstimmung bestehe, halte man die Beschlußempfehlung für unzureichend. Hinsichtlich des Beschlußempfehlungsvorschlags der Fraktion DIE GRÜNEN gebe es Überschneidungen. Einige Punkte seien jedoch dort nicht so differenziert dargestellt, wie man es sich z. B. hinsichtlich der Bereiche APIS und NADIS vorstelle. Der Beschlußempfehlungsvorschlag der Fraktion der SPD enthalte demgegenüber die Punkte, die eine bedeutende Rolle in den Berichterstattergesprächen und in den Ausschußberatungen gespielt hätten. Man habe auf die Punkte verzichtet, in denen ein gewisses Entgegenkommen der Bundesregierung oder eine gewisse Übereinstimmung vorgelegen habe.

Die Fraktion DIE GRÜNEN lehnte den Antrag der Koalitionsfraktionen bis auf die Punkte 2 und 3 ab, zu denen sie sich bei Einzelabstimmungen der Stimme enthalten hätte, und erklärte, der Beschlußempfehlungsvorschlag der Fraktion der SPD enthalte mehr Parallelen zu dem der Fraktion DIE GRÜNEN als der Koalitionsantrag.

3. Zur Beschlußempfehlung im einzelnen

Im folgenden wird dargelegt, inwieweit die Beschlußempfehlungsvorschläge der Oppositionsfraktionen mit der Beschlußempfehlung übereinstimmen. Zudem werden die in den Ausschußdiskussionen und Berichterstattergesprächen vertretenen Standpunkte zu den in der Beschlußempfehlung aufgegriffenen Themen wiedergegeben und aufgeführt, inwieweit die Voten der mitberatenden Ausschüsse Berücksichtigung gefunden haben.

Im übrigen wird auf die Oppositionsanträge unter Ziffer 4 dieses Berichts eingegangen.

3.1 Zu Nummer 1

Nummer 1 der Beschlußempfehlung betrifft die vom Bundesbeauftragten in den Kapiteln 6.4.1, 6.7 und 6.8 des Achten Tätigkeitsberichts und Kapiteln 8.3 und 8.5 des Neunten Tätigkeitsberichts angesprochenen Themen. Sie entspricht Empfehlungen des Ausschusses für das Post- und Fernmeldewesen.

Die Fraktion der SPD hat sich dem Votum des Ausschusses für das Post- und Fernmeldewesen ebenfalls angeschlossen.

Die Fraktion DIE GRÜNEN hat in ihrem Beschlußvorschlag gleichfalls die Themen „Weitergabe der Anschriften von Postkunden an die Deutsche Postreklame", „Zwangseintragung der Teilnehmer/innen am öffentlichen Fernsprechnetz in das Telefonbuch", „Übermittlung der Anschriften von z. B. Neugeborenen und Konfirmanden zu Werbezwecken durch Postzustellerinnen" aufgegriffen und Forderungen hierzu aufgestellt (siehe hierzu Ziffer 4.2 dieses Berichts).

3.2 Zu Nummer 2

Nummer 2 der Beschlußempfehlung betrifft Kapitel 5 — hier insbesondere Punkt 5.1.1 — des Achten Tätigkeitsberichts und Kapitel 7 — hier insbesondere Punkt 7.1.2 — des Neunten Tätigkeitsberichts und greift z. T. die Stellungnahme des Ausschusses für Arbeit und Sozialordnung auf.

Die Fraktion der SPD fordert in ihrem Beschlußempfehlungsentwurf unter Ziffer IV gleichfalls, die Beihil-

festellen von der allgemeinen Personalverwaltung strikt abzutrennen.

Der Beschlußempfehlungsvorschlag der Fraktion DIE GRÜNEN enthält in Parallele zu Nummer 2 der Beschlußempfehlung die Anregung an die Bundesregierung, unverzüglich den Entwurf einer bereichsspezifischen Regelung des Arbeitnehmer/innen-Datenschutzes vorzulegen, wie sie es u. a. in ihrer Stellungnahme zum Achten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz angekündigt habe. Zudem enthält ihr Beschlußempfehlungsvorschlag zahlreiche Vorschläge für Regelungen, die der Entwurf enthalten müsse. Im Rahmen der Beratungen im Innenausschuß wurde von der Fraktion DIE GRÜNEN zudem erklärt, man stimme der Forderung nach einer Abschottung der Beihilfestellen von der Personalverwaltung zu.

Die Bundesregierung wies im Rahmen der Beratungen darauf hin, daß ein Gesetz über das Personalaktenrecht geplant sei, das noch in dieser Legislaturperiode verabschiedet werden solle und zur Frage der Trennung von Beihilfestellen und Personalstellen im einzelnen Stellung nehme. Ein Beschluß, der schon vorab zur Trennung der Bereiche auffordere, sei willkommen. Derzeit sei die Vertraulichkeit der Beihilfeakten im Dienstrecht niedergelegt. Lediglich in sehr kleinen Behörden ergäben sich insoweit manchmal Probleme.

3.3 *Zu Nummer 3*

Die Beschlußempfehlung betrifft unter Nummer 3 ein in Kapitel 18.3 des Neunten Tätigkeitsberichts angesprochenes Thema und greift das Votum des mitberatenden Ausschusses für Jugend, Familie, Frauen und Gesundheit auf.

Die Fraktion der SPD hat diesem Votum ausdrücklich zugestimmt.

Die Fraktion DIE GRÜNEN hat in ihrem Beschlußempfehlungsvorschlag mehrere darüber hinausgehende Aufforderungen zum Thema Eignungs- und Verwendungsprüfungen aufgestellt (siehe hierzu Ziffer 4.2 dieses Berichts).

3.4 *Zu Nummer 5*

Nummer 5 der Beschlußempfehlung betrifft eine vom Bundesbeauftragten für den Datenschutz unter Ziffer 13.1 seines Neunten Tätigkeitsberichts angesprochene Problematik: Nach Ziffer 8.1 der Dateienrichtlinien sind zu löschende Daten auf dem jeweiligen Datenträger unkenntlich zu machen. Die hierzu geführten Unterlagen sind zu vernichten.

Im Verlauf der Beratungen kam zwischen dem Bundesbeauftragten für den Datenschutz und der Bundesregierung keine Einigung darüber zustande, auf welche Weise bei Unterlagen, die sowohl zu löschende als auch weiterhin zu speichernde Daten enthalten, verfahren werden solle. Nach Ansicht des Bundesbeauftragten für den Datenschutz ist als Minus zu der Dienstanweisung zumindest zu verlangen, daß Informationen in Akten mit einem Stempelaufdruck gekennzeichnet und damit der weiteren Verwertung entzogen werden, wenn die dazu gehörige Datenspeicherung inzwischen gelöscht wurde.

Seitens der Bundesregierung wurde für ausreichend gehalten, daß die Ursprungsmeldung mit einem entsprechenden Trennblatt versehen aufbewahrt werde.

Die Fraktion der SPD hat in den Ausschußberatungen ebenso wie die Koalitionsfraktionen das Petitum des Bundesbeauftragten für den Datenschutz unterstützt. Sie hat zu diesem Thema einen der Beschlußempfehlung der Koalitionsfraktionen inhaltlich entsprechenden Beschlußempfehlungsvorschlag eingereicht (siehe Ziffer VIII c des unter Ziffer 4.1 wiedergegebenen Beschlußempfehlungsvorschlags der Fraktion der SPD).

Die Fraktion DIE GRÜNEN betonte im Rahmen der Beratungen, es gehe nicht an, kleine Verbesserungen anzubringen, wenn die bisherige Art und Weise der Erfassungen und Speicherungen beim Bundeskriminalamt fortgesetzt werde. Es sei vorab zu erwähnen, wie viele Personen in Dateien bezüglich Rauschgiftkriminalität gespeichert seien, um das Ausmaß der Datensammlung deutlich zu machen: In der Falldatei Rauschgift seien Daten über 200 000 Beschuldigte oder Verdächtige und insgesamt 270 000 Fälle gespeichert. In der Arbeitsdatei PIOS-Rauschgift seien Daten über 70 000 Personen gespeichert, davon über 500 über „andere Personen" (Neunter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz). Diese Zahlen machten deutlich, daß bei der Speicherung nicht unterschieden werde, ob es sich um bloße Konsumenten von Betäubungsmitteln handele, bezüglich deren Daten die Fraktion DIE GRÜNEN eine Speicherung uneingeschränkt ablehne, oder um Großdealer mit kriminellen Praktiken. Die Fraktion kritisierte, daß selbst Minimalforderungen des Bundesbeauftragten für den Datenschutz nicht stattgegeben werde, und betonte zudem, daß die grundsätzliche Kritik der Fraktion DIE GRÜNEN am Bundeskriminalamt mit seinen Praktiken bezüglich der Datenerhebung, -speicherung, -weitergabe und -löschung von den in diesem Bericht abgegebenen Stellungnahmen der Fraktion unberührt bleibe.

3.5 *Zu Nummer 6*

Der Bundesbeauftragte für den Datenschutz vertritt in Kapitel 13.1 seines Neunten Tätigkeitsberichts die Ansicht, daß der Personendatensatz, der wegen der geringen Schwere des Delikts nicht im überregionalen allgemeinen Kriminalaktennachweis (KAN), sondern lediglich in der sachbezogenen „Falldatei Rauschgift" gespeichert werden dürfe, auch nur dem Zugriff von Polizeidienststellen unterliegen dürfe, die mit der Bekämpfung der Rauschgiftkriminalität befaßt seien. Im Innenausschuß führte er hierzu aus, neben der Falldatei Rauschgift sei eine Notierung in INPOL vorhanden, die auf die Tatsache einer Erfassung in der Falldatei Rauschgift im Einzelfall hinweise. Der Hinweis werde nicht nur der mit Rauschgift befaßten Stelle zugänglich gemacht, sondern über INPOL jeder an INPOL angeschlossenen Dienststelle zugänglich.

Im Rahmen der Beratungen im Innenausschuß legte die Bundesregierung dar, daß nach verschiedenen Abfragemöglichkeiten zu differenzieren sei. Eine Abfragemöglichkeit sei auf eine Personengesamtauskunft gerichtet. Eine andere Abfragemöglichkeit laufe auf eine KAN-Auskunft hinaus. Bei letzterer sei noch nicht vorgesehen, die Falldatei Rauschgift auszuklammern. Man habe aber die Absicht, dies zu tun. Beim Abfragen des Kriminalaktennachweises (KAN) werde künftig kein Hinweis mehr auf vorhandenen Datenbestand in der Falldatei Rauschgift (FDR) ausgegeben werden, sofern keine KAN-Relevanz der FDR-Fälle (überregionale Bedeutung, schwere Straftat) gegeben sei.

Die Koalitionsfraktionen begründeten ihre in der Beschlußempfehlung enthaltene Auffassung damit, daß man es wegen des engen Zusammenhanges zwischen Rauschgiftkriminalität und Beschaffungskriminalität für erforderlich halte, die bisherige Praxis beizubehalten, um auch solchen Polizeidienststellen, die nicht unmittelbar mit Rauschgift zu tun hätten, den Zugriff weiterhin zu ermöglichen.

Die Fraktion der SPD wünschte, daß der seitens des Bundesbeauftragten für den Datenschutz beanstandete Mangel bald behoben und dem Innenausschuß hierüber berichtet werde.

Die Fraktion DIE GRÜNEN betonte, daß das Prinzip der Zweckbindung Beachtung finden müsse.

3.6 Zu Nummer 7

Das Problem der Speicherung dritter Personen in Dateien des Bundeskriminalamts wurde im Innenausschuß insbesondere im Zusammenhang mit den Speicherungen in APIS erörtert. Insoweit geht die Beschlußempfehlung auf die Ausführungen des Bundesbeauftragten für den Datenschutz in Kapitel 13.3, 1. bis 3. Spiegelstrich des Neunten Tätigkeitsberichts zurück. Im Rahmen der Beratungen im Innenausschuß führte der Bundesbeauftragte für den Datenschutz ergänzend aus, bei Einspeicherungen in APIS würden schwere terroristische Straftaten und allgemeine Kriminalität bis hin zur Kleinkriminalität in einen Topf geworfen. Dies bewirke eine Eingriffserweiterung. Formen der Datenverarbeitung, die speziell für die Bekämpfung des Terrorismus entwickelt worden seien, würden auf die gesamte Staatsschutzkriminalität ausgeweitet. Ein Beispiel für diese Vermischung seien die Daten der „L-Gruppe". Es handele sich hierbei um detaillierte personenbezogene Merkmale. Die Errichtungsanordnung für APIS sehe die Speicherung von Daten der L-Gruppe unterschiedslos für alle Personen vor. Selbst über „andere Personen", d. h. Kontakt- und Randpersonen, könnten danach Persönlichkeitsprofile gespeichert werden. Für die Speicherung dieser „anderen Personen" fehle eine Rechtsgrundlage. Er wiederholte seine Kritik auf Seite 12 seines gesonderten Prüfberichts über die Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamts.

Seitens der Bundesregierung wurde demgegenüber betont, daß nur besonders qualifizierte Kleinkriminalität in APIS gespeichert werde. Im Gesetz über das Bundeskriminalamt finde sich die Rechtsgrundlage für die Speicherungen in APIS. Sie umfasse auch die Speicherung „anderer Personen". Es handele sich hierbei um Personen, die in relevantem Zusammenhang zu einer gravierenden Straftat — z. B. einem Delikt i. S. d. § 129a oder § 138 StGB — stünden. Es würden keine Persönlichkeitsprofile erstellt, sondern nur Merkmale des äußeren Erscheinungsbildes festgehalten. In einer Recherchedatei könne man auf Personenbeschreibungen nicht verzichten. Es werde jedoch erwogen, nur noch die äußeren Merkmale, die in der Erscheinung lägen, zu speichern und auf die Merkmale, die unter „Verhalten" genannt seien, zu verzichten, obwohl manche dieser Merkmale kriminalistisch durchaus einen Sinn hätten.

Die Fraktion der SPD unterstützte die Kritik des Bundesbeauftragten für den Datenschutz, indem sie erklärte, die Zusammenfassung schwerer terroristischer Straftaten und allgemeiner Kriminalität bis hin zur Kleinkriminalität verletze den Grundsatz der Verhältnismäßigkeit und der Erforderlichkeit. Die Errichtungsanordnung für APIS, in der die unterschiedslose Speicherung von Daten der L-Gruppe auch für Nicht-Verdächtige vorgesehen sei, sei rechtswidrig.

Diese Auffassung spiegelt sich auch in Nummer IX des Beschlußempfehlungsvorschlags der Fraktion der SPD nieder (siehe dazu Ziffer 4.1.9 dieses Berichts zum Thema Erfassung von Kleinkriminalität in APIS).

Die Fraktion DIE GRÜNEN bemängelte, daß für die Speicherung „anderer Personen" in APIS die Rechtsgrundlage fehle. In ihrem Beschlußempfehlungsvorschlag stellte die Fraktion DIE GRÜNEN bezüglich APIS zudem fest, daß die Einbeziehung „anderer Personen" und „Gefährdeter" und deren potentielle minutiöse Personenbeschreibung den Verhältnismäßigkeitsgrundsatz verletze.

3.7 Zu Nummer 8

Nummer 8 der Beschlußempfehlung bezieht sich insbesondere auf in Kapitel 13.3 des Neunten Tätigkeitsberichts aufgeführte Bedenken des Bundesbeauftragten für den Datenschutz. Im Rahmen der Beratungen beanstandete er, daß das föderative Prinzip dadurch berührt werde, daß jeder Teilnehmer an APIS befugt und verpflichtet sei, an von anderen Teilnehmern eingestellten Datensätzen unmittelbar Veränderungen oder Ergänzungen vorzunehmen. Die strukturellen Grundlagen der Datenverarbeitungen würden im Verhältnis von Bund und Ländern nachhaltig verändert, ohne daß der Gesetzgeber tätig geworden sei. Gegen den Betrieb von Verbundsystemen bestünden keine grundsätzlichen organisations- oder datenschutzrechtlichen Bedenken, sofern die Rechtsgrundlagenproblematik gelöst sei. Entscheidende Fragen seien, ob vorgegebene Verantwortungsgrenzen eingehalten und ob die Verantwortlichkeiten hinreichend klar definiert und sachgerecht aufgeteilt worden seien. Problematisch sei die Übernahme von Daten(mit)verantwortung ohne eine vorhergehende Zulässigkeitsprüfung hinsichtlich derjenigen Daten innerhalb der Datengruppe, die im Rahmen der eigenen

Tätigkeit nicht angefallen seien. Insbesondere sei die Befugnis zur Änderung und Löschung der im Mitbesitz befindlichen Daten problematisch. Änderungen und Löschungen erfolgten unmittelbar mit Wirkung für alle Verbundteilnehmer. Wenn ein Mitbesitzer eine Information lösche, weil er sie nicht mehr für speicherwürdig halte, könne ein anderer Mitbesitzer dazu eine andere Auffassung haben.

Für die Beurteilung sei es wesentlich, daß der Verbund nicht mehr allein der wechselseitigen Informationsbereitstellung diene, sondern auch eine wechselseitige Beteiligung an der Aufgabenerfüllung umfasse, nämlich an der Pflege der eigenen Daten. Die wechselseitige Änderungsbefugnis markiere den Übergang vom Informationsverbund zum Aufgabenverbund und bedürfe daher einer besonderen Rechtfertigung. Durch eine Verfügung über Daten eines anderen Teilnehmers könne dessen Verwaltungshandeln wesentlich vorherbestimmt werden. Die APIS-Verbundteilnehmer hätten vereinbart, bei „wesentlichen" Änderungen die Mitbesitzer der betreffenden Daten zu benachrichtigen. Dies erscheine aber nicht ausreichend. Zunächst sei schwer zu bestimmen, was eine „wesentliche" Änderung sei. Auch kleine Änderungen könnten erhebliche Konsequenzen haben. Die Wesentlichkeit werde sich oft erst aus der Sicht des Empfängers ergeben. Es bestehe auch die Gefahr, daß Benachrichtigungen versehentlich oder aus Zeitmangel unterblieben. Schließlich sei gezielter Mißbrauch möglich. Die Tatsache, daß alle Änderungen automatisch protokolliert würden, löse das Problem nicht, da die Protokolldaten sachlich und zeitlich nur beschränkt zur Verfügung stünden. Verfassungsrechtlich erscheine diese Datenorganisation unter den Gesichtspunkten des Ressortprinzips (Artikel 65 GG) und der parlamentarischen Ministerverantwortlichkeit problematisch. Eine umfassende Verantwortung des Bundesministers des Innern für die Aufgabenerfüllung des Bundeskriminalamtes sei schwer denkbar, wenn Stellen außerhalb des Geschäftsbereichs wesentliche Eingriffe in die Daten vornehmen könnten, die die Grundlage der Amtstätigkeit bildeten. Bedenken gegen die Datenorganisation bestünden auch unter dem Gesichtspunkt der bundesstaatlichen Ordnung. Ein direkter Eingriff des Bundes in Datenbestände eines Landes oder umgekehrt sei eine Form der Beeinflussung des Verwaltungshandelns, für die eine verfassungsrechtliche Legitimation nicht ersichtlich sei. Die Verwaltungskompetenz nach Artikel 87 Satz 2 GG (Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen, für die Kriminalpolizei) dürfte das Verfahren nicht decken, soweit es über den Informationsaustausch hinausgehe. Von der Gesetzgebungskompetenz nach Artikel 73 Nr. 10 GG (Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei) werde nicht in einschlägiger Weise Gebrauch gemacht; es müßte auch näher untersucht werden, in welchem Umfang auf dieser Grundlage durch einfaches Gesetz Mischverwaltung zwischen Bund und Ländern begründet werden dürfe. Zum Schutz der informationellen Selbstbestimmung bedürfe ein Verbundsystem vom Typ APIS präziser bereichsspezifischer gesetzlicher Grundlagen, die insbesondere den Informationsfluß berechenbar machten und die Verantwortlichkeit für Grundrechtseinschränkungen klar zuordneten. Jede Polizeibehörde sei dafür verantwortlich, daß die von ihr angelegten Vorgänge einschließlich der Datenspeicherungen nach angemessenen Fristen darauf überprüft würden, ob sie vernichtet bzw. gelöscht werden könnten. In der Praxis der polizeilichen Datenverarbeitung würden jedoch — zumindest in Teilbereichen — die wegen Fristablaufs gebotenen Aussonderungsprüfungen nicht durchgeführt, wenn zur selben Person von einem anderen Teilnehmer eine noch andauernde Aussonderungsprüffrist vergeben worden sei. Auch dabei handele es sich der Sache nach um eine Delegation von Verantwortung, denn die speichernde Stelle überlasse es einem anderen Teilnehmer, zu entscheiden, daß ihre Unterlagen samt Datenspeicherung aufrechterhalten blieben. Im Einzelfall könne zwar ein polizeilicher Vorgang eines anderen Teilnehmers durchaus eine weitere Aufbewahrung rechtfertigen, etwa wenn ein Sachzusammenhang bestehe. Eine pauschale, rechnergesteuerte Abhängigkeit bedeute jedoch, daß die speichernde Stelle ihre Verantwortung nicht wahrnehme und die Entscheidung über die Aufbewahrungsdauer anderen Stellen überlasse, die bei ihrer Entscheidung diese Nebenfolge jedoch in keiner Weise einbezögen und auch nicht einbeziehen könnten. Auch für die Frage der Fristensteuerung gelte daher, daß eine Aufgabenwahrnehmung im Verbund eine Form der Mischverwaltung darstelle, die jedenfalls einer besonderen Rechtfertigung bedürfe.

Nach Auffassung der Bundesregierung kann man, selbst wenn man das Führen von Verbunddateien i. S. v. Nummer 2.1 der Dateienrichtlinien als spezielle Erscheinungsform einer Mischverwaltung bezeichnen wollte, in der darin liegenden Zusammenarbeit zwischen Bund und Ländern keine mit den Artikeln 83 ff. GG unvereinbare Form gemeinsamer Verwaltungstätigkeit sehen. Es gebe keinen allgemeinen verfassungsrechtlichen Grundsatz, wonach Verwaltungsaufgaben ausschließlich vom Bund oder von den Ländern wahrzunehmen seien, sofern nicht ausdrücklich verfassungsrechtliche Regelungen etwas anderes zuließen. Eine ausdrückliche Regel des Verfassungsrechts, wonach eine Verbunddatei nach Art von APIS ausgeschlossen sein müßte, gebe es nicht. Eine verwaltungsorganisatorische Erscheinungsform sei nicht deshalb verfassungswidrig, weil sie als Mischverwaltung einzuordnen sei, sondern nur, wenn ihr zwingende Kompetenz- oder Organisationsnormen oder sonstige Vorschriften des Verfassungsrechts entgegenstünden. Mit einer Verbunddatei i. S. d. Nummer 2.1 der Dateienrichtlinien werde nicht sachwidrig in Landesbefugnisse eingegriffen, sondern eine für eine wirksame Verwaltungstätigkeit des Bundes auf der Grundlage des Artikel 87 Abs. 1 GG einerseits sowie der Länderpolizeien andererseits unerläßliche Voraussetzung geschaffen. Zudem sei nach Artikel 73 Nr. 10 i. V. m. Artikel 87 Abs. 1 Satz 2 GG eine „Koordinierungsverwaltung" gerade zulässig. Probleme betreffend eine Kenntlichmachung der Verantwortlichkeit für die Einspeicherungen könnten gelöst werden, indem die Protokollbänder, aus denen der Verantwortliche ersehbar sei, länger aufbewahrt würden.

Die Koalitionsfraktionen führten zur Begründung ihrer Beschlußempfehlung an, überwiegend würden von den Ländern Daten in APIS eingestellt, zum Teil jedoch auch vom Bundeskriminalamt selbst. Wenn sich z. B. herausstelle, daß ein Datum, das von einem Bundesland eingegeben worden sei, falsch sei und ein anderes Bundesland dies feststelle, sei letzteres berechtigt, dieses Datum zu ändern. Man halte dies für problematisch insbesondere auch deshalb, weil später nicht mehr feststellbar sei, wer verantwortlich für das Datum in der geänderten Fassung sei. Man wisse nicht mehr, wer es geändert habe, und warum er es geändert habe. Damit sei die rechtliche und politische Verantwortlichkeit für das Datum nicht mehr erkennbar. Beides müsse aber z. B. im Hinblick auf mögliche Schadensersatzansprüche erkennbar sein.

Die Fraktion der SPD vertrat die Ansicht, zum Schutz der informationellen Selbstbestimmung bedürfe ein Verbundsystem vom Typ APIS präziser bereichsspezifischer gesetzlicher Grundlagen, die den Informationsfluß berechenbar machten und die Verantwortlichkeit für Grundrechtseinschränkungen klar zuordneten. Solange diese Grundfragen nicht gelöst seien, sei APIS einzustellen; zumindest sei die gegenseitige Änderungsbefugnis zu beenden.

Die Fraktion DIE GRÜNEN brachte in den Innenausschuß einen Beschlußempfehlungsvorschlag ein, in dem sie bemängelte, das Betreiben einer redundanzfreien Polizei-Verbunddatei auf Bundesebene widerspreche dem föderalen Prinzip und der ausschließlichen Landeszuständigkeit in Polizeisachen, da die durch einzelne Länder angelieferten Daten nicht eigenständig verwaltet würden.

3.8 Zu Nummer 9

Nummer 9 der Beschlußempfehlung bezieht sich auf Seite 45 und Seite 46 der Stellungnahme der Bundesregierung zum Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz. Über den Umfang der Aktualisierungspflicht hinsichtlich der in APIS gespeicherten Daten vertraten der Bundesbeauftragte für den Datenschutz und die Bundesregierung unterschiedliche Auffassungen.

Im Rahmen der Berichterstattergespräche wies der Bundesbeauftragte für den Datenschutz darauf hin, daß den Bundeskriminalämtern in der Regel nur die Einleitung eines Ermittlungsverfahrens gemeldet werde, nicht aber dessen Abschluß bzw. die spätere gerichtliche Behandlung des Falles. Deshalb seien die meisten Kriminalakten des Bundeskriminalamtes insofern unvollständig. Er verwies auf seinen bereits mehrfach gemachten Vorschlag, daß spätestens nach drei Jahren die Kriminalakten zur Wiedervorlage gelangen sollten. Da beim Bundeskriminalamt für minderschwere Fälle inzwischen ohnehin eine dreijährige Speicherfrist gelte, würde dies bei der großen Mehrzahl der nach drei Jahren vorgelegten Akten ohnehin zu deren Vernichtung und zur Löschung der zugehörigen Speicherung führen. Lediglich bei den schweren Fällen, die länger als drei Jahre gespeichert bleiben müßten, solle dann aktiv bei der meldenden Landespolizeidienststelle nachgefragt werden, was aus dem eingeleiteten Verfahren bzw. dem geäußerten Verdacht inzwischen geworden sei. Der Bundesbeauftragte für den Datenschutz verwies darauf, daß eine solche Verfahrensweise auch Vorteile aus der Sicht der Polizei biete. Stelle sich durch aktive Nachfrage bei den Landespolizeibehörden heraus, daß ein ursprünglich gemeldeter Verdacht sich als haltlos erwiesen habe, führe dies zur Löschung und damit auch zur Freisetzung von Rechnerkapazitäten. Außerdem könne man dann bei eiligen Anfragen auf vollständige Unterlagen zurückgreifen und müsse sich nicht erst unter Zeitdruck nach dem Ausgang eines Ermittlungsverfahrens erkundigen. Der Bundesbeauftragte für den Datenschutz betonte, man könne nicht davon ausgehen, daß erst im Falle einer Weitergabe der Daten an Dritte ein Eingriff erfolge. Vielmehr stelle die Speicherung in den Dateien des Bundeskriminalamtes für sich gesehen einen Eingriff dar. Dies gelte insbesondere, solange Staatsschutzfälle noch in der Datei der Verfassungsschutzbehörden NADIS gespeichert würden. Hierdurch würden diese Daten auch an alle Verfassungsschutzbehörden weiter übermittelt. Es komme deshalb darauf an, daß der in dieser Speicherung liegende Eingriff auf einem Sachverhalt beruhe, der ihn tatsächlich rechtfertige.

Das Bundeskriminalamt habe die Pflicht, durch eigene Erkundigungen festzustellen, ob ein derartiger Sachverhalt tatsächlich vorliege. Der Bundesbeauftragte für den Datenschutz wies darauf hin, daß sein Vorschlag, eine derartige Erkundigung erst nach drei Jahren vorzunehmen, bereits einen Kompromiß darstelle. Er habe dabei in Rechnung gestellt, daß die große Mehrzahl der bei der Abteilung Staatsschutz gespeicherten Fälle ohnehin nach drei Jahren zu löschen sei. Er sei deshalb davon ausgegangen, daß die Arbeitsbelastung, die hierdurch für das Bundeskriminalamt entstünde, in einem angemessenen Verhältnis zu den schutzwürdigen Belangen der Betroffenen stehe. Im Hinblick auf die vom Bundeskriminalamt auch gegen diesen Vorschlag geltend gemachte Frage der Arbeitskapazität schloß sich der Bundesbeauftragte für den Datenschutz dem von mehreren Berichterstattern gemachten Vorschlag an, zumindest für die Zukunft eine dreijährige Wiedervorlagefrist für alle Fälle vorzusehen und sich dann nach Ablauf dieser Frist aktiv nach dem Stand des Verfahrens zu erkundigen.

Seitens der Bundesregierung wurde angeführt, daß dem Bundesbeauftragten für den Datenschutz bereits folgende Vorschläge zur Behebung des Problems gemacht worden seien: Zum einen solle, wenn ein Vorgang zur Bearbeitung beim Bundeskriminalamt anstehe, die Stelle, die die Vorgänge übermittelt habe, gebeten werden, über den Ausgang des Strafverfahrens zu berichten. Zum anderen solle das Bundeskriminalamt, wenn es die ihm übermittelten Informationen weitergebe, die Stelle, die die Vorgänge übermittelt habe, darauf hinweisen, daß auch die Stelle, an die die Informationen weiterübermittelt würden, über den Ausgang des Verfahrens informiert werden müsse. Dieser Vorschlag sei dem Bundesbeauftragten für den Datenschutz nicht weit genug gegangen. Hinsichtlich des Vorschlags des Bundesbeauftragten für den Datenschutz, daß das Bundeskriminalamt vor der Weitergabe von Informationen den Ausgang des Ver-

fahrens prüfen müsse, wurde erwidert, daß zur polizeilichen Aufgabenerfüllung ein schneller Informationsfluß notwendig sei. Die Daten würden jedoch in dem Moment, in dem sie Verwendung fänden, aktualisiert und seien vorher nicht relevant. Eine Löschung erfolge, sobald die meldende Stelle beispielsweise über die Einstellung des Verfahrens informiere. Eine Pflicht, das Bundeskriminalamt über Veränderungen zu informieren, ergebe sich aus den Richtlinien für den polizeilichen Meldedienst in Staatsschutzsachen, deren Befolgung unterstellt werden müsse. Für das Bundeskriminalamt bestehe zudem die Verpflichtung, nachzufragen, ob auch alle Veränderungen mitgeteilt worden seien. Die Einführung einer generellen Vorlagefrist von drei Jahren bedeute demgegenüber einen erheblichen Arbeitsaufwand. Unter Zugrundelegung einer Stichprobe ergebe sich: Mit einer Aufarbeitung der gesamten St-Altbestände wären sieben Personen ein Jahr lang beschäftigt. Die laufende Bearbeitung der Kriminalakten mit dreijähriger Wiedervorlagefrist würde eine Arbeitskraft erfordern. Ein weiterer Aufwand würde bei den Stellen entstehen, die zusätzlich eingeschaltet werden müßten. Dies seien insbesondere die Staatsschutzbereiche der Landeskriminalämter. Nach dem derzeitigen Verfahren — Aktualisierung dann, wenn mit den Daten gearbeitet werde und der mit der Speicherung vorhandene Eingriff sich konkretisiere — trete eine Verpflichtung zur Aktualisierung wesentlich seltener ein, als bei einer pauschalen Überprüfung. Man halte es weiterhin für ausreichend, wenn die Aktualitätsprüfung jeweils im Rahmen der Sachbearbeitung erfolge. Denn solange die Akten ruhten, sei die Intensität des Eingriffs so gering, daß nicht jede Akte immer wieder überprüft werden müsse. Zudem bestehe auch bei Einführung einer dreijährigen Wiedervorlagefrist lediglich die Chance, daß die Akten vollständiger seien, aber nicht die Sicherheit der Vollständigkeit, da unmittelbar nach Durchführung der Wiedervorlageprüfung Änderungen eintreten könnten.

Seitens der Koalitionsfraktionen wurde darauf hingewiesen, daß man umfangreiche Diskussionen über die Wiedervorlagefristen geführt habe. Sie vertraten die Meinung, daß es möglich sein müsse, bezogen auf APIS für alle Delikte in gleicher Weise eine dreijährige Wiedervorlagefrist einzuführen, mit dem Ziel, alle drei Jahre zu überprüfen, ob die Speicherung noch berechtigt sei, oder ob Ereignisse eingetreten seien, die es erforderlich machten, die Speicherung zu löschen. Es liege auch im Interesse der Funktionsfähigkeit der Dateien, den Datenbestand so klein wie möglich zu halten.

Die Fraktion der SPD nahm in ihrem Beschlußempfehlungsvorschlag unter Ziffer VIII b zu diesem Themenkomplex Stellung (siehe Ziffer 4.1 dieses Berichts). Sie wies im Rahmen der Beratungen im Innenausschuß ausdrücklich darauf hin, daß die Drei-Jahres-Frist nicht nur — anders als die Koalitionsfraktionen es forderten — für die Daten, die in APIS gespeichert seien, gelten solle, sondern für alle Staatsschutzakten und -dateien. Es gehe nicht nur um die Frage der formalen Überprüfung, weil diese den zuständigen Beamten dazu verleiten könne, die Laufzeiten zu verlängern. Er müsse gezwungen sein, Fragen nach dem Stand des Verfahrens zu stellen und daraufhin eine Löschung der Daten bzw. eine Veränderung der gespeicherten Daten vorzunehmen. Die Frage der entsprechenden Organisation müsse noch einmal geklärt werden. Man habe relativ gute Erfahrungen mit einer Sondergruppe gemacht, die mit der Überprüfung der Akten beauftragt werde. Im übrigen seien entsprechend den vom Bundesbeauftragten für den Datenschutz auf Seite 15 seines zusätzlichen Berichts über die datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamtes aufgestellten Empfehlungen die bei den einzelnen APIS-Teilnehmern vorhandenen Kriminalakten selbständig zu betrachten und nach den für den jeweiligen Teilnehmer gültigen KpS-Richtlinien zu behandeln.

Die Fraktion DIE GRÜNEN kritisierte, daß die Bundesregierung selbst den Mindestforderungen des Bundesbeauftragten für den Datenschutz nicht nachkomme. Sie beanstandete in ihrem Beschlußempfehlungsvorschlag insoweit hinsichtlich der Datei APIS, daß Datenschutz und Datenrichtigkeit organisatorisch nicht gewährleistet seien, z. B. wegen des Fehlens von Nachberichtspflichten und wegen unvollständiger Auskunftserteilung gegenüber den betroffenen Bürgern und Bürgerinnen.

3.9 *Zu Nummer 10*

Nummer 10 der Beschlußempfehlung geht auf die Ausführungen des Bundesbeauftragten für den Datenschutz in Kapitel 13.2 seines Neunten Tätigkeitsberichts zum Thema „Weitere Zunahme der SPUDOK-Anwendungen" zurück.

Im Rahmen der Berichterstattergespräche führte der Bundesbeauftragte für den Datenschutz ergänzend aus, SPUDOK-Dateien würden in immer größerem Umfang benutzt. Bei ihrer Errichtung werde häufig sehr flüchtig gearbeitet, was ein Indiz dafür sei, daß diese Dateien sehr schnell errichtet würden. Teilweise gehe aus den Errichtungsanordnungen nicht klar genug hervor, wie der betroffene Personenkreis einzugrenzen sei. Zum Teil würden SPUDOK-Dateien zudem bereits zur Bewertung von Gefahrensituationen errichtet. Notwendig seien eine restriktive Handhabung hinsichtlich der Errichtung der SPUDOK-Dateien und eine präzise Arbeit bei der Aufstellung der Errichtungsanordnungen. Der Gesetzgeber müsse in diesem Bereich tätig werden. Es wies darauf hin, daß nicht immer der Meldepflicht nach § 19 Abs. 4 BDSG genügt worden sei. Zudem werde der Grundsatz, der für „andere Personen" in den Dateienrichtlinien hinsichtlich der Auskunftserteilung über gespeicherte Daten aufgestellt sei, bei SPUDOK-Dateien vernachlässigt. Er fragte zudem, warum die Datei CHECK-LOG neben APIS erforderlich sei, da die Speicherung von Daten gefährdeter Personen bereits in der Datei APIS erfolge, und schlug vor, die Beratungen über die mit SPUDOK zusammenhängenden Fragen fortzusetzen, sobald der vom Bundesminister des Innern in Aussicht gestellte zusammenfassende Bericht über die Entwicklung der elektronischen Datenverarbeitung beim Bundeskriminalamt vorliege. Im Rahmen der Beratungen im Innenausschuß fügte er klarstellend hinzu, er habe die Existenz von SPUDOK-Dateien nicht in Frage gestellt, sondern formelle Anstöße

dahin gehend genommen, daß Dateien nicht ordnungsgemäß gemeldet worden seien. Letzteres sei inzwischen bereinigt worden. Man habe gemeinsam mit dem Bundeskriminalamt auch in einer anderen Frage einen vernünftigen Weg gefunden:

In den SPUDOK-Dateien würden auch Daten Nichtbeschuldigter gespeichert, falls Hinweise auf einschlägige Verbindungen bestünden. Unter Umständen könne die Aufklärung einer Tat durch solche Hinweise ermöglicht werden. Es gehe hauptsächlich darum, daß die Informationen ganz genauen Zweckbeschränkungen unterliegen müßten. Dies habe das Bundeskriminalamt zugesagt. Damit sei man einen wesentlichen Schritt zum Schutz der Bürger vorangekommen.

Die Bundesregierung legte demgegenüber dar, der Sinn der SPUDOK-Dateien bestehe jeweils darin, für Ermittlungsverfahren, bei denen in großem Umfang Informationen anfielen, diese Informationen bereitzuhalten. Diese würden im Laufe des Ermittlungsverfahrens ausgewertet und nach dessen Abschluß gelöscht, oder gesperrt, wenn die Informationen beispielsweise wegen des Berufungsverfahrens erhalten bleiben müßten. Bei Ermittlungsverfahren, die untereinander in engem Zusammenhang stünden, werde es für vernünftig gehalten, diese in einer gemeinsamen Datei zu erfassen. Die Errichtungsanordnungen für die SPUDOK-Dateien müßten aufgrund der notwendigerweise schnellen Errichtung der Dateien vielfach schematisch formuliert werden. Die Zahl der Verfahren, bei denen es sinnvoll sei, die Ermittlungen durch SPUDOK zu unterstützen, sei gestiegen. Seit Mai 1987 seien drei neue SPUDOK-Dateien eingerichtet und zwei gelöscht worden. Unter Gesichtspunkten des Datenschutzrechts sei es sinnvoller, mehrere kleine Dateien zu haben als große Falldateien. Der sich aus § 19 Abs. 4 BDSG ergebenden Meldepflicht werde vorrangig nachgekommen. Soweit Mängel hinsichtlich der Errichtungsanordnung einzelner SPUDOK-Dateien bestünden, sei man sehr bemüht, diese abzustellen. Es erfolgten hier auch Unterweisungen innerhalb des Bundeskriminalamtes in Abstimmung mit dem Bundesminister des Innern. Die die Datei CHECKLOG betreffende Errichtungsanordnung würde derzeit zwischen dem Bundesminister des Innern und dem Bundeskriminalamt abgestimmt. Die Speicherungen in CHECKLOG erfolgten aus organisatorischen Gründen, um die Datei APIS nicht zusätzlich zu belasten. Es seien nur in Ausnahmefällen die Voraussetzungen für eine Doppelspeicherung gegeben. Das Bundeskriminalamt vertrete den Standpunkt, daß die Unterrichtung einer gefährdeten Person wegen geringer Eingriffsqualität nicht erfolgen solle, um den Betreffenden nicht zu beunruhigen. Das zuständige Referat des Bundesministeriums des Innern halte die Unterrichtung demgegenüber für erforderlich. Die Rechtsgrundlage für die Errichtung der SPUDOK-Dateien ergebe sich zur Zeit aus § 2 BKAG i. V. m. § 9 BDSG. Ein Entwurf zu einem Bundeskriminalamtgesetz solle noch in diesem Jahr dem Kabinett zugeleitet werden. Es sei davon auszugehen, daß im Bundeskriminalamtgesetz und in der Strafprozeßordnung in Zukunft Bestimmungen über die Errichtungsanordnungen enthalten sein würden.

Die Koalitionsfraktionen betonten, daß SPUDOK-Dateien für einzelne Ermittlungsverfahren angelegt würden, und sahen insoweit keine gravierenden Probleme. Zur Ermittlung schwerwiegender konkreter Straftaten sei das SPUDOK-Verfahren heute unerläßlich. Es seien beachtliche Erfolge hierdurch erzielt worden. Das Verfahren müsse fortbestehen, wenn man eine Aufklärung dieser Straftaten u. U. auch zugunsten der Opfer erreichen wolle. Die Kritik könne allenfalls hinsichtlich einer Anwendung des Systems, die nicht zur Aufklärung konkreter Ermittlungsverfahren erfolge, angebracht werden.

Die Fraktion der SPD vertrat die Ansicht, SPUDOK-Anwendungen seien äußerst restriktiv vorzunehmen. Nur unbedingt erforderliche Anwendungen seien zulässig, bis Regelungen im Bundeskriminalamtgesetz bzw. in der Strafprozeßordnung beschlossen seien. Die Bundesregierung solle den Bericht über die Gesamtentwicklung der automatisierten Datenverarbeitung im Bundeskriminalamt vorlegen.

Die Fraktion DIE GRÜNEN wandte sich gegen das Sammeln von personenbezogenen Daten auf Vorrat für den Fall, daß die eine oder andere Person eventuell irgendwann einmal kriminell werden könnte. Der Bundesminister des Innern müsse aufgefordert werden, den zusammenfassenden Bericht über die Entwicklung der elektronischen Datenverarbeitung beim Bundeskriminalamt bald vorzulegen.

4. Alternativen

4.1 Beschlußempfehlungsvorschlag der Fraktion der SPD

Der mit den Stimmen der Koalitionsfraktionen gegen die Stimmen der Fraktion der SPD bei Enthaltung der Fraktion DIE GRÜNEN mehrheitlich abgelehnte Vorschlag der Fraktion der SPD für die Beschlußempfehlung hatte insgesamt folgenden Wortlaut:

„I. Zu 1.3 Übergangsbonus

Der Übergangsbonus ist abgelaufen. Spätestens Ende dieser Legislaturperiode werden verstärkt verfassungsrechtliche Konflikte auftreten. Die Bundesregierung wird aufgefordert, noch in dieser Legislaturperiode dem Parlament alle Gesetze zum Beschluß vorzulegen, die aufgrund des Volkszählungsurteils des Bundesverfassungsgerichts novelliert werden müssen.

II. Zu 1.7 Die Dienststelle

Die Aufgaben des Bundesbeauftragten für den Datenschutz sind durch neue Gesetze, aber auch durch die vehemente Entwicklung neuer Technologien in großem Umfang gewachsen. Um eine ausreichende Kontrollfähigkeit des BfD zu erhalten bei vorhandenen und neu einzurichtenden Dateien, müssen dem Bundesbeauftragten für den Datenschutz seine Stellenforderungen erfüllt werden.

III. Zu 4. Rechtswesen

Der Innenausschuß stellt fest, daß die Vorschläge und Beanstandungen immer noch nicht umgesetzt sind und fordert die Bundesregierung auf, unverzüglich tätig zu werden. Insbesondere sind die Vorlagen für das Justizmitteilungsgesetz, das Bundeszentralregistergesetz und die Vorschriften über das Schuldnerverzeichnis bis zum 1. September 1988 vorzulegen. Die weiteren bereichsspezifischen Datenvorschriften sollen bis spätestens ein Jahr vor Ablauf der Wahlperiode vorgelegt sein.

IV. Zu 7. Personalwesen

Zu 7.1.2 Beihilfe

Die Beihilfestellen müssen von der allgemeinen Personalverwaltung strikt abgetrennt werden.

Zu 7.1.3 Besoldung/Versorgung

Die Kindergeldakten im Bundesministerium des Innern und seinem Geschäftsbereich müssen separat geführt werden. Sie dürfen nicht dem Kostenteil der Personalakte zugeordnet werden.

V. Zu 8. Deutsche Bundespost

Der BfD hat das Recht, mit den Personalvertretungen bei den Behörden unmittelbar Verbindung aufzunehmen, und umgekehrt hat die Personalvertretung das Recht, sich unmittelbar an den BfD zu wenden.

VI. Zu 9.3 Kfz-Zulassungsdaten

Die Zusatzerhebungen der Zulassungsstellen bei Kfz-Anmeldungen bei Ausländern werden unverzüglich eingestellt.

VII. Zu 12. Öffentliche Sicherheit

Zu 12.3 Neufassung der Sicherheitsüberprüfungsrichtlinien

Für die Sicherheitsüberprüfungsrichtlinien fehlt nach wie vor die gesetzliche Grundlage. Bei den neuen Sicherheitsüberprüfungsrichtlinien wird der Grundsatz der Zweckbindung der im Rahmen einer Sicherheitsüberprüfung erhobenen Daten zwar ausdrücklich festgeschrieben; zugleich sind aber Ausnahmen in derart weitem Umfang vorgesehen, daß das Prinzip in nicht akzeptabler Weise ausgehöhlt wird. Deswegen fordert der Innenausschuß, daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten nur zum Zwecke der Sicherheitsüberprüfung verwendet werden dürfen. Ausnahmen sind allenfalls für die gleichen Zwecken dienende Spionageabwehr möglich.

VIII. Zu 13. Bundeskriminalamt

a) Speicherung personengebundener Hinweise (PHW)

   Die Speicherungen personengebundener Hinweise im Aktennachweissystem sind grundsätzlich abzulehnen. Personengebundene Hinweise sind nur mit ganz engen Einschränkungen in Fahndungsdateien zulässig und möglichst ganz aufzugeben. Ausnahme: Der personengebundene Hinweis „bewaffnet".

   Kurze Überprüfungsfristen sind speziell für diese Daten einzuführen. Am Beispiel des PHW für HIV-Infizierte zeigt sich ganz besonders die Fragwürdigkeit dieses Instruments. PHW sind für HIV-Infizierte grundsätzlich abzulehnen.

b) Die Bundesregierung wird aufgefordert, für alle im Staatsschutzbereich gespeicherten Datensätze eine Wiedervorlagefrist von drei Jahren einzuführen mit dem Ziel, nach Ablauf der Frist die Erforderlichkeit der weiteren Speicherung zu prüfen und sich insbesondere nach dem Ausgang eingeleiteter Ermittlungsverfahren zu erkundigen.

c) Darüber hinaus ist die Aktualisierung von Datensätzen ein generelles Problem, das nach wie vor im BKA ungelöst ist. Insbesondere im Umgang mit Unterlagen, die sowohl zu löschende als auch weiterhin zu speichernde Daten enthalten, sind die zu löschenden Daten durch Stempelaufdrucke gemäß den Dateirichtlinien unkenntlich zu machen.

IX. Zu 13.3 Inbetriebnahme der Datei APIS

Die Zusammenfassung schwerer terroristischer Straftaten und allgemeiner Kriminalität bis hin zur Kleinkriminalität verletzt den Grundsatz der Verhältnismäßigkeit und der Erforderlichkeit und ist deswegen einzustellen. Die Erfassung der Kleinkriminalität in APIS ist unzulässig. Wenn 70 Prozent der Speicherungen über den Auffangtatbestand erfolgen, wird die Ausnahme zur Regel. Der Hinweis, viele Terroristen hätten im Bereich der Kleinkriminalität angefangen, kann derartige Speicherungen nicht legitimieren.

Auf die Motivation des Täters abzustellen ist nicht zulässig. Die Errichtungsanordnung muß konkretisiert werden. „Andere Straftaten" dürfen in APIS nur erfaßt werden, wenn sie in der Schwere mit den genannten Straftaten vergleichbar sind.

Da dies bisher nach wie vor ungeklärt ist, beschließt der Ausschuß, die Speicherung in APIS bis auf weiteres einzustellen.

Der Innenausschuß beschließt, Bundesregierung und Länder, BKA und die LKA aufzufordern, Speicherungen in APIS bis zur endgültigen Klärung einzustellen. Die Problematik wird besonders deutlich dadurch, daß in der Errichtungsanordnung für APIS die unterschiedslose Speicherung von Daten der L-Gruppe auch für Nichtverdächtige vorgesehen ist. Das ist rechtswidrig. Zum Schutz der informationellen Selbstbestimmung bedarf ein Verbundsystem vom Typ APIS präziser bereichsspezifischer gesetzlicher

Grundlagen, die den Informationsfluß berechenbar machen und die Verantwortlichkeit für Grundrechtseinschränkungen klar zuordnen.

Solange diese Grundfragen nicht gelöst sind, ist die Speicherung in APIS auszusetzen.

X. Zugriff der Teilnehmer an NADIS auf die Fundstellen von Akten der Abteilung ST des BKA

Das Bundeskriminalamt hat die Nutzung des nachrichtendienstlichen Informationssystems NADIS als Aktennachweissystem für seine Abteilung Staatsschutz nicht eingestellt. Die Benutzung von NADIS durch das BKA hat den datenschutzrechtlichen bedenklichen Effekt, daß die anderen Teilnehmer an NADIS (Bundesamt für Verfassungsschutz, Landesämter für Verfassungsschutz; MAD und BND im Wege des Bandabgleichs) direkten Zugriff auf die Fundstellen des Bundeskriminalamtes haben. Hier wird auch das Trennungsgebot verletzt. Der weitere Zugriff auf NADIS ist rechtswidrig und nach gültigem Bundesdatenschutzgesetz unzulässig. Deswegen ist der Zugriff auf NADIS unverzüglich einzustellen.

XI. 14. Bundesamt für Verfassungsschutz (BfV)

Datenübermittlung vom BfV an ausländische Nachrichtendienste

Die Erhebung, Verarbeitung und Weitergabe personenbezogener Informationen durch das BfV ist nur zulässig im Rahmen der sich aus § 3 des Verfassungsschutzgesetzes ergebenden Zwecke. Die Sicherheitsinteressen ausländischer Daten gehören zu diesen Zwecken nicht, auch nicht das Interesse der Bundesrepublik Deutschland, im Wege des Datenaustauschs von ausländischen Staaten Informationen zu erhalten, die im Rahmen der Zwecke des § 3 Bundesverfassungsschutzgesetz liegen. Daraus folgt, daß de lege lata die Weitergabe von personenbezogenen Informationen an ausländische Dienste schlechthin unzulässig ist. Ob und in welchem Umfang es de lege ferenda erforderlich ist, die Weitergabe von persönlichen Informationen zuzulassen (z. B. bei NATO-Partnern oder bei anderen EG-Staaten, die in Sicherheitsinteressen mit den unseren so verknüpft sind, daß sie wie unsere eigenen behandelt werden müssen), wird die Bundesregierung im Rahmen der Novellierung des Verfassungsschutzgesetzes darzulegen und zu begründen haben.

Die Stelle, bei der angefragt wird, muß davon unterrichtet werden, daß die Anfrage durch ein Auskunftsersuchen eines ausländischen Nachrichtendienstes veranlaßt worden ist. Außerdem muß das BfV von sich aus überprüfen, ob es insbesondere inländische Gesetzes- oder Dienstvorschriften gibt, die einer Weitergabe entgegenstehen. Ein Rundschreiben an ausländische Nachrichtendienste mit dem Hinweis, daß im Rahmen von Sicherheitsüberprüfungen, an denen das BfV mitgewirkt hat, den Betroffenen Gelegenheit gegeben werden müsse, sich zu den vom BfV übermittelten Informationen zu äußern, ist unzureichend. Es bietet nicht die Gewähr, daß entsprechend verfahren wird. Dieses Risiko wird auch nicht ausgeschlossen, wenn in jedem Einzelfall bei der Übermittlung von Erkenntnissen an ausländische Dienste im Rahmen von Sicherheitsüberprüfungen auf das Rundschreiben erneut hingewiesen wird.

XII. 20. Datensicherung

Die Bundesregierung wird aufgefordert, einen Gesamtbericht über den Einsatz von Personalcomputern in den Bundesverwaltungen zu geben, unter Berücksichtigung des Berichtes des Bundesrechnungshofes zu diesem Bereich."

Im folgenden wird auf die Diskussion des Beschlußempfehlungsvorschlags der Fraktion der SPD im Innenausschuß eingegangen, soweit dies nicht bereits unter Ziffer 3 dieses Berichts geschehen ist.

4.1.2 Zu Nummer I

Die Fraktion der SPD verzichtete im Innenausschuß auf eine Beratung des Themenbereichs „Übergangsbonus", nachdem seitens der Bundesregierung die Zeitpläne betreffend das Gesetz über das Ausländerzentralregister, das Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, das Änderungsgesetz über den Bundesgrenzschutz, das Geheimschutzgesetz, das Gesetz über die Bevölkerungsstatistik, das Justizmitteilungsgesetz, das Bundeszentralregistergesetz, das Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis und die Strafprozeßordnung vorgelegt worden waren.

4.1.3 Zu Nummer III

Der Beschlußempfehlungsvorschlag entspricht in Nummer III einem im Rechtsausschuß mehrheitlich abgelehnten Antrag der Fraktion der SPD.

Seitens der Koalitionsfraktionen wurde dem Beschlußempfehlungsvorschlag zugestimmt, jedoch angeregt, den Termin „1. September 1989" durch das Wort „unverzüglich" zu ersetzen. Sie betonten, Eile sei zudem hinsichtlich einer Reform der Strafprozeßordnung, des Gesetzes über das Bundeskriminalamt und des Änderungsgesetzes über den Bundesgrenzschutz unter datenschutzrechtlichen Aspekten geboten.

4.1.4 Zu Nummer IV

Die Fraktion DIE GRÜNEN stimmte dem Beschlußempfehlungsvorschlag der Fraktion der SPD zur Kindergeldaktenführung zu.

4.1.5 Zu Nummer V

Der Beschlußempfehlungsvorschlag der Fraktion der SPD geht in Nummer V auf die Bitte des Ausschusses für das Post- und Fernmeldewesen zurück, zu klären, ob der Bundesbeauftragte für den Datenschutz das Recht habe, mit den Personalvertretungen bei den Behörden unmittelbar Verbindung aufzunehmen.

Der Bundesbeauftragte für den Datenschutz hielt diese Frage für sehr bedeutsam, da sich häufig Personalvertretungen zwecks Beratung an ihn wendeten. Er werde zudem oftmals bei Streitigkeiten zwischen den Personalvertretungen und den Dienstherrn durch die Einigungsstellen hinzugezogen. Nach seiner Auffassung ist der Personalrat ein vom Gesetz mit eigenen Rechten und Pflichten angestatteter „jedermann" i. S. d. § 21 BDSG. In der Praxis nehme man natürlich auf die Situation der Dienststellen Rücksicht und versuche, Probleme mit der Dienststelle gemeinsam zu erörtern. Bei einem Wunsch des Personalrats nach Beratung in der Dienststelle unterrichte man den Dienstherrn vorher hiervon. Eine Umfrage unter den Länderdatenschutzbeauftragten habe ergeben, daß gegenüber nicht einem einzigen Landesdatenschutzbeauftragten seitens einer Behörde das Recht der Personalvertretung bestritten worden sei, sich an den jeweiligen Datenschutzbeauftragten zu wenden. In einem einzigen Fall sei seitens einer Behörde geäußert worden, der Datenschutzbeauftragte dürfe sich erst gegenüber dem Personalrat kritisch äußern, wenn vorher die Dienststelle mit dieser Kritik befaßt worden sei. Es gehe letzten Endes um die Frage, ob die Personalvertretungen legitimiert seien, das Recht auf informationelle Selbstbestimmung mitzuwahren oder nicht.

Die Bundesregierung führte demgegenüber aus, es sei zwischen der datenschutzrechtlichen und der personalvertretungsrechtlichen Seite zu differenzieren. Jedermann i. S. d. § 21 BDSG sei jede natürliche Person. Der Personalrat sei eine spezielle Personenvereinigung und Teil der Dienststelle. Insoweit sei er nicht „jedermann" i. S. des BDSG. Die Personalvertretung werde vom Gesetzgeber als Bestandteil der Dienststelle gesehen, die in der Dienststelle mit der Dienststelle zusammenarbeiten müsse. Eine enge Zusammenarbeit der Personalvertretung mit den Datenschutzbeauftragten oder einer anderen Dienststelle außerhalb der eigenen sei gesetzlich nicht vorgesehen. Die Bundesregierung verwies auf eine Stellungnahme von Prof. Dr. Maihofer aus dem Jahre 1978, in der ausgeführt sei, daß eine Personalvertretung nicht eigene Rechte außerhalb des Bereichs der Dienststelle habe. Das Bundesverfassungsgericht habe zwar inzwischen in diesem Bereich eine Fortentwicklung bewirkt, aber auch danach seien Verfassungsbeschwerden von Personalvertretungen zurückgewiesen worden. Man schlage vor, abzulehnen, daß ohne Wissen der Dienststelle der Bundesbeauftragte für den Datenschutz direkt Kontakt mit den Personalvertretungen aufnehme.

Die Fraktion der SPD betonte, daß es nur im Bereich der Deutschen Bundespost in dieser Frage Schwierigkeiten gebe. Die Möglichkeit eigenständigen Verhaltens müsse für den Bundesbeauftragten für den Datenschutz und die Personalvertretungen auch im Bereich der Deutschen Bundespost gegeben sein. Die Arbeitnehmerrechte müßten in Sachen Datenschutz auch im kollektivrechtlichen Bereich verstärkt werden. Die Inhalte der Beratungen der Personalräte mit dem Bundesbeauftragten für den Datenschutz müßten den Dienststellen nicht bekannt sein.

Die Koalitionsfraktionen betonten, auch wenn man die Personalvertretungen als Teil der Dienststelle betrachte, müsse der Datenschutzbeauftragte mit ihnen direkt in Kontakt treten können. Vorauszusetzen sei allerdings, daß die oberste Dienststelle hiervon in Kenntnis gesetzt sei. Sie schlugen vor, zur Abklärung der Rechtslage ein Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages anzufordern.

Dieses Gutachten gelangte zu dem Ergebnis, den Personalvertretungen stehe das Anrufungsrecht des § 21 Bundesdatenschutzgesetz nicht zu. Sie dürften jedoch nach dem Bundespersonalvertretungsgesetz (BPersVG) ohne vorherige Einschaltung der Dienststelle vom Bundesbeauftragten Informationen und Auskünfte einholen. Hinweise auf Mißstände seien jedoch an die Voraussetzung des § 66 Abs. 3 BPersVG gebunden. Danach dürften außenstehende Stellen erst angerufen werden, wenn eine Einigung in der Dienststelle nicht erzielt worden sei. Der Bundesbeauftragte für den Datenschutz dürfe sich demgegenüber unmittelbar an die Personalvertretungen wenden.

Die Fraktion DIE GRÜNEN fordert in ihrem Beschlußempfehlungsvorschlag die Bundesregierung auf, den direkten Zugang des Bundesbeauftragten für den Datenschutz zu den Personalvertretungen der Postbehörden zu gewährleisten. Sie betonte, der Datenschutz müsse so ernst genommen werden, daß alle Betroffenen das Recht und die Pflicht hätten, sich um Verstöße zu kümmern.

4.1.6 Zu Nummer VI

Die Bundesregierung stellte im Rahmen der Beratungen im Innenausschuß zum Thema „Zusatzerhebungen der Zulassungsstellen bei Kfz-Anmeldungen von Ausländern" klar, die Angelegenheit sei inzwischen bereinigt: Das Gesetz zur Änderung des Straßenverkehrsgesetzes habe für die Tätigkeit des Zentralen Fahrzeugregisters beim Kraftfahrtbundesamt und auch für die örtlichen Fahrzeugregister eine datenschutzrechtliche Grundlage geschaffen. In den einschlägigen Vorschriften sei nicht vorgesehen, daß in den Fahrzeugregistern Paßdaten und die Heimatanschrift von Ausländern gespeichert werden sollten. Einvernehmen mit den Ländern sei dahin gehend erzielt worden, daß die Länder insgesamt auf die Erhebung und Speicherung dieser Daten verzichteten.

4.1.7 Zu Nummer VII

Zur Begründung ihres Beschlußempfehlungsvorschlags zum Thema „Neufassung der Sicherheitsüberprüfungsrichtlinien" führte die Fraktion der SPD aus, der Übergangsbonus sei abgelaufen, so daß die

rechtliche Grundlage für die Sicherheitsüberprüfungsrichtlinien fehle. Man begrüße zwar, daß durch die Neufassung der Sicherheitsüberprüfungsrichtlinien Verbesserungen erzielt worden seien; diese seien jedoch nicht ausreichend. Problematisch sei z. B. die Einbeziehung der Verwandten und des Umfeldes, in dem jemand lebe, und die Anwendung der Sicherheitsrichtlinien auf den Deutschen Bundestag und die Mitarbeiter des Deutschen Bundestages.

Die Koalitionsfraktionen vertraten demgegenüber die Auffassung, daß die derzeitige Praxis vom Übergangsbonus gedeckt sei, weil Sicherheitsüberprüfungen unerläßlich seien, um ein Mindestmaß an Sicherheit in der öffentlichen Verwaltung sicherzustellen. Ein Geheimschutzgesetz, das für die Zukunft eine Rechtsgrundlage schaffe, müsse bald in Kraft treten.

Die Fraktion DIE GRÜNEN lehnte die Durchführung von Sicherheitsüberprüfungen generell ab und erklärte, daran ändere sich auch nichts in dem Fall, daß eine gesetzliche Grundlage hierfür geschaffen werde. Die Überprüfungen dienten der Erstellung von Persönlichkeitsbildern.

4.1.8 Zu Nummer VIII a)

Nummer VIII des Beschlußempfehlungsvorschlags bezieht sich hinsichtlich des Themas „Speicherung personengebundener Hinweise" auf die Ausführungen des Bundesbeauftragten für den Datenschutz unter Nummer 13.1 seines Neunten Tätigkeitsberichts. Soweit der Beschlußempfehlungsvorschlag sich auf die Speicherung des personengebundenen Hinweises, (PHW) ANST-Vorsicht Blutkontakte, der Auskunft über eine HIV-Infektion gibt, bezieht, wird auf Drucksache 11/4232 verwiesen: Im Rahmen des Berichts des Innenausschusses zu dem Antrag der Fraktion DIE GRÜNEN, Dateispeicherungspraxis beim BKA, hier: Hinweis auf HIV-Infizierte — Drucksache 11/1157 — wurden insoweit die Beratungen des Innenausschusses zum Achten und Neunten Tätigkeitsbericht sowie die Berichte einbezogen, die die Bundesregierung am 22. Juni und 12. Oktober 1988 zum Thema „Speicherung HIV-Infizierter in INPOL" vor dem Innenausschuß abgegeben hat. Zudem wurden die Diskussionen, die über diese Berichte stattfanden und die Anträge, die in diesem Rahmen gestellt wurden, einbezogen.

Der Innenausschuß hat sich über die neuesten Entwicklungen im gesamten Bereich, der Speicherung personengebundener Hinweise jeweils durch die Bundesregierung informieren lassen. Mit Schreiben vom 24. Mai 1988 berichtete die Bundesregierung, nach den geltenden Errichtungsanordnungen erfolge die Speicherung gegenwärtig in folgenden Dateien: In den Dateien Personenfahndung, Kriminalaktennachweis, Erkenntnisdienst, Haftdatei und Falldatei Rauschgift würden die personengebundenen Hinweise „bewaffnet", „gewalttätig", „Ausbrecher", „BTM-Konsument" und „Freitodgefahr" gespeichert. Der personengebundene Hinweis „Ansteckungsgefahr" werde in den Dateien Personenfahndung, Kriminalaktennachweis und der Falldatei Rauschgift und die personengebundenen Hinweise „geisteskrank" und „Prostitution" in der Datei Personenfahndung und der Falldatei Rauschgift geführt. Der Arbeitskreis II habe zum Umfang der zulässigen Katalogbegriffe und zur Regelung des Datenfeldes PHW am 1./2. Februar 1988 mehrheitlich einen Beschluß gefaßt, der im Hinblick auf Zulässigkeit, Anwendungsbezogenheit und Speicherungsdauer eine unterschiedliche Praxis in den Ländern bewirkt hätte. Die Konferenz der Innenminister und -senatoren der Länder (IMK) habe daraufhin in ihrer Sitzung am 28./29. April 1988 den Arbeitskreis II gebeten, die Angelegenheit mit dem Ziel, eine möglichst einheitliche Speicherungspraxis zu erreichen, erneut zu beraten. Der Arbeitskreis II habe sich in einer Sondersitzung am 10./11. Mai 1988 mit der Angelegenheit befaßt und eine Arbeitsgruppe unter Vorsitz von Rheinland-Pfalz und Beteiligung des Bundes und aller Länder eingesetzt. Die Arbeitsgruppe, die sich mit der Gesamtproblematik der Speicherung von personengebundenen Hinweisen in INPOL einschließlich des Hinweises auf eine HIV-Infizierung befassen solle, sei gebeten worden, alsbald ein Ergebnis vorzulegen. Aus technischen Gründen sei derzeit nicht in allen Fällen gewährleistet, daß die den PHW einspeichernde Stelle aus dem Datensatz ersichtlich sei, und der PHW bei einer INPOL-Abfrage nur aus den Dateien übermittelt werde, in denen er geführt werden dürfe. Zur Zeit werde in der AG-Kripo geprüft, inwieweit durch Einrichtung einer eigenen Datengruppe für die PHW (W-Gruppe) sichergestellt werden könne, daß die für die Einstellung verantwortliche Stelle aus dem Datensatz ersichtlich sei. Die erforderlichen dv-technischen Vorkehrungen für eine anwendungsbezogene Nutzung würden nach entsprechender Beschlußfassung in den Gremien der IMK bei einer Betriebssystemumstellung beim Bundeskriminalamt zu realisieren sein. Mit Schreiben vom 13. September 1988 teilte die Bundesregierung mit, die vom Arbeitskreis II eingesetzte Bund/Länder-Arbeitsgruppe habe am 1. August 1988 einen Beschlußvorschlag abgegeben, dem der Arbeitskreis II in seiner Sitzung am 6./7. September gefolgt sei.

Der Beschluß des Arbeitskreises II habe folgenden Wortlaut:

„I.

1. Der AK II hält die Verwendung personengebundener Hinweise im Zusammenhang mit der Erfüllung polizeilicher Aufgaben für erforderlich.
2. Die zugelassenen personengebundenen Hinweise werden in den Anwendungen KAN, Personenfahndung, ED-Datei und in der Falldatei Rauschgift geführt.

   Die Nutzung personengebundener Hinweise in der Haftdatei wird eingestellt.

   Das KAN-Konzept und die Errichtungs-/Feststellungsanordnungen für INPOL-Bund-Anwendungen sind entsprechend zu ändern.
3. Die personengebundenen Hinweise „Land-/Stadtstreicher" (LAST) und „häufig wechselnder Aufenthaltsort" (HWAO) entfallen.

4. Folgende PHW sind weiterhin zugelassen:

   BEWA = bewaffnet
   GEWA = gewalttätig
   AUSB = Ausbrecher
   ANST = Ansteckungsgefahr
   GEKR = geisteskrank
   BTMK = BTM-Konsument
   FREI = Freitodgefahr
   PROS = Prostitution

5. Die Speicherung von Hinweisen auf HIV-Infektionen ist in das Ermessen des Bundes und jedes Landes gestellt.

   Sofern der Bund oder ein Land die Speicherung dieser Hinweise vornehmen, erfolgen sie, mit Ausnahme der Laufzeit, nach den gleichen Kriterien wie die der übrigen Hinweise auf Ansteckungsgefahr.

6. Für die Vergabe personengebundener Hinweise gelten die in der Anlage zum Beschluß des AK II vom 1./2. Februar 1988, TOP 6 beschriebenen Kriterien.

7. Die Übermittlung personengebundener Hinweise erfolgt auf der Grundlage gesetzlicher Regelungen bzw. der KpS-Richtlinien. Sie ist nur zu dem Zweck zulässig, zu dem die Speicherung erfolgt ist. Dem Grundsatz der Erforderlichkeit kommt hierbei besondere Bedeutung zu.

   Es ist DV-technisch sicherzustellen, daß ein PHW bei einer INPOL-Abfrage tatsächlich nur aus den Dateien übermittelt wird, in denen er — laut Errichtungsanordnung — auch geführt werden darf.

8. Durch DV-technische Vorkehrungen ist sicherzustellen, daß die Herkunft eines PHW aus dem Datensatz direkt ersichtlich ist. Die AG Kripo wird gebeten, umgehend die hierfür erforderlichen DV-technischen Voraussetzungen zu schaffen.

9. Es werden folgende Laufzeiten für die PHW festgelegt:

   BEWA, GEWA, AUSB, BTMK, ANST (Vorsicht Blutkontakte) für die Dauer der Aufbewahrung der KpS des Betroffenen,

   PROS 5 Jahre,
   ANST, FREI 2 Jahre.

II.

Der AK II empfiehlt der Innenministerkonferenz folgende Beschlußfassung:

Die Innenministerkonferenz nimmt den Beschluß des AK II zustimmend zur Kenntnis."

Der Stimme enthalten hätten sich: Hamburg, Hessen, Niedersachsen. Gegen den Beschluß hätte Baden-Württemberg gestimmt.

Mitgeteilt wurden als Anlage zu dem Beschluß folgende Kriterien für die Vergabe personengebundener Hinweise:

Bewaffnet (BEWA)

darf nur vergeben werden, wenn Anhaltspunkte dafür vorliegen, daß

— der Betroffene eine Waffe im technischen Sinne (vgl. u. a. §§ 244, 250 StGB) bei der Begehung einer Straftat verwendet hat,

  oder

— er eine Waffe zur Begehung von Straftaten, insbesondere um sich einer Festnahme zu widersetzen, mit sich führen wird.

Gewalttätig (GEWA)

darf nur vergeben werden, wenn Anhaltspunkte dafür vorliegen, daß der Betroffene zukünftig bei Straftaten, insbesondere Widerstandshandlungen, erhebliche körperliche Gewalt gegen Personen oder Sachen einsetzen wird.

Ausbrecher (AUSB)

darf nur vergeben werden, wenn der Betroffene schon einmal aus amtlichem Gewahrsam entwichen ist oder sich dem Vollzug der Freiheitsentziehung mit Gewalt widersetzt hat oder beim Vollzug der Freiheitsentziehung geflohen ist.

Ansteckungsgefahr (ANST)

darf nur vergeben werden, wenn ärztliche oder amtliche Hinweise oder Angaben des Betroffenen selbst vorliegen,

— daß der Betroffene unter einer nach § 3 Abs. 1 und 2 Bundesseuchengesetz meldepflichtigen Krankheit leidet oder

— daß der Betroffene gemäß § 2 dieses Gesetzes krank, krankheitsverdächtig, ansteckungsverdächtig, Ausscheider oder ausscheidungsverdächtig ist und eine Ansteckung eine schwerwiegende Gesundheitsgefährdung bedeuten würde.

Auf die Art der Krankheit ist hinzuweisen. Bei HIV-Infektion erfolgt dies durch den Zusatz „Vorsicht Blutkontakte".

Geisteskrank (GEKR)

darf nur vergeben werden, wenn ärztlich festgestellt ist, daß der Betroffene an einer Geisteskrankheit leidet.

BTM-Konsument (BTMK)

darf nur vergeben werden, wenn Anhaltspunkte dafür vorliegen, daß der Betroffene mißbräuchlich

— Opiate jeder Art, z. B. Heroin-, Codein-, Morphin-Zubereitungen,

— Kokain,

— Amphetamine (sogenanntes Speed),

— Halluzinogene, z. B. Cannabis-Präparate, LSD, Meskalin,

— alle anderen ärztlich gebrauchten Betäubungsmittel

verbraucht, gleichgültig, ob diese Mittel eingenommen, geschnupft oder injiziert werden.

Als BTM-Konsument gilt auch, wer anstelle der o. a. Stoffe sogenannte Ausweichmittel mißbräuchlich konsumiert, z. B. Fortral, Valoron-N, Captagon, Ephedrin-Präparate oder dgl.

Freitodgefahr (FREI)

darf nur vergeben werden, wenn Anhaltspunkte dafür vorliegen, daß der Betroffene den Freitod suchen könnte, wobei für die Prognose ein zurückliegender Freitodversuch von Bedeutung sein kann.

Prostitution (PROS)

darf nur vergeben werden, wenn gesicherte Erkenntnisse darüber vorliegen, daß

— eine weibliche Person ihren Lebensunterhalt überwiegend aus der Gewerbsunzucht bestreitet (Prostituierte)

oder

— eine männliche Person — vorwiegend im Straßen- oder Lokalstrich — ihren Lebensunterhalt überwiegend aus der Gewerbsunzucht bestreitet (Strichjunge).

In der Sitzung des Innenausschusses am 12. Oktober 1988 legte die Bundesregierung dar, die Innenministerkonferenz habe sich am 6./7. Oktober 1988 mit dem Bereich der personengebundenen Hinweise insgesamt befaßt. Auf der Grundlage von Vorschlägen des Arbeitskreises II sei die Zahl der zugelassenen personengebundenen Hinweise gestrafft worden. Es seien künftig nicht mehr die bisherigen Zuspeicherungen Land-/Stadtstreicher und HWAO — häufig wechselnder Aufenthaltsort — enthalten. Es würden datenverarbeitungstechnische Vorkehrungen gefordert, die sicherstellen sollten, daß die personengebundenen Hinweise bei einer INPOL-Anfrage nur aus den Dateien übermittelt würden, in denen sie geführt würden. Außerdem solle sichergestellt werden, daß die Herkunft des personengebundenen Hinweises unmittelbar aus dem Datensatz ersichtlich sei.

Der Bundesbeauftragte für den Datenschutz vertrat im wesentlichen die Positionen, die in dem Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. November 1985 zur Speicherung personengebundener Hinweise im INPOL-System (Drucksache 10/4690 S. 72) enthalten sind und bemängelte, daß der Beschluß der Innenministerkonferenz in wesentlichen Punkten davon abweiche.

Die Koalitionsfraktionen vertraten die Ansicht, personengebundene Hinweise dienten insgesamt nicht der Stigmatisierung, sondern hätten den Sinn, Polizeibeamte bzw. Betroffene zu schützen. Über die Geeignetheit des Mittels ließe sich zwar streiten. Zudem sei die Handhabung der Speicherung und des Abrufs im einzelnen zu überprüfen. Abzustellen sei jedoch darauf, was zum Schutz Festgenommener oder zum Schutz der Polizeibeamten erforderlich sei: So sei z. B. die Speicherung des Merkmals Freitodgefahr sinnvoll, um Selbstmorde in Streßsituationen, z. B. vor einer Verhaftung oder im Fall der Inhaftierung, verhindern zu können. Die Kriterien für das Vorliegen der personengebundenen Hinweise seien vom Arbeitskreis II detailliert festgelegt worden.

Die Fraktion DIE GRÜNEN forderte bundesweit die Löschung von personengebundenen Hinweisen in Dateien, da diese lediglich der Stigmatisierung der Betroffenen dienten. Durch die Speicherungen würden scheinbar von der Norm abweichende Personengruppen erfaßt. Das Merkmal PROS z. B. ermögliche die Erfassung einer Gruppe aufgrund ihres Gewerbes. Das Speicherungsmerkmal Freitodgefahr sei völlig überflüssig. Die Polizisten müßten immer von einer belastenden Situation für die Beteiligten ausgehen und entsprechend geschult sein, um in den konkreten Situationen Selbstmorde verhindern zu können. Das Personal in Haftanstalten müsse sich entsprechend um die Inhaftierten kümmern.

4.1.9 Zu Nummer IX

Nummer IX des Beschlußempfehlungsvorschlags, der sich auf die Inbetriebnahme der Datei APIS bezieht, geht auf die Ausführungen des Bundesbeauftragten für den Datenschutz in Kapitel 13.3 seines Neunten Tätigkeitsberichts zurück sowie auf die Ergänzungen in Kapitel III seines zusätzlichen Prüfberichts über die datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamtes.

Die Bundesregierung legte gegenüber der Kritik des Bundesbeauftragten für den Datenschutz dar, APIS sei die automatisierte Form des Meldedienstes und diene der Abwehr und Verhütung von Gefahren. Aufgrund dieser Datei seien Hinweise an die Polizei darüber möglich, von wem Gefahren ausgingen. Es handele sich um eine wichtige Recherchedatei, ohne die die Bekämpfung der Terrorismus- und Staatsschutzkriminalität sehr erschwert werde. Es gehe hierbei sowohl um Verhütung als auch um Aufklärung dieser Kriminalität. Diese Datei werde für unerläßlich i. S. der Rechtsprechung des Bundesverfassungsgerichts zum Übergangsbonus gehalten. In APIS seien etwa 15 000 Beschuldigte und etwa 10 000 Verdächtige gespeichert. Dies dürfte etwa ⅕ der in den Verfassungsschutzberichten registrierten Mitglieder in extremistischen Organisationen entsprechen, ohne den orthodox-kommunistischen Block. Zudem seien „andere Personen" gespeichert. Hinsichtlich der Speicherungskriterien legte sie dar, die derzeit in der Errichtungsanordnung enthaltene Fassung sei so konkret wie möglich. Es seien zudem genügend Anweisungen vorhanden, um eine einheitliche Handhabung in den Ländern zu gewährleisten. Kriterium für eine Speicherung sei eine verfassungsfeindliche Zielsetzung,

die mit Kriminalität in Verbindung treten müsse. Daher könne man nicht von einer Gesinnungsdatei reden. Bei organisierten Verbrechen sei eine täterbezogene Sicht nötig. Die Motivation des Täters komme als ein zusätzliches Kriterium hinzu, das eine große Bedeutung habe. Eine Speicherung müsse schon im Bereich der Einstiegskriminalität erfolgen. Viele Terroristen hätten im Bereich der Kleinkriminalität angefangen. Eine Erfassung lediglich der schweren Kriminalität erfolge zu spät. Eine Abgrenzung könne allein im Bereich der Löschungsfristen erfolgen. Die Anzahl der beispielsweise im Zusammenhang mit der Volkszählung erfaßten Delikte habe aufgrund etlicher Löschungen erheblich abgenommen. In den Fachgremien sei in den Gesprächen von Bund und Ländern eine Reduzierung des Straftatenkataloges des kriminalpolizeilichen Meldedienstes und der Errichtungsanordnung von APIS strikt abgelehnt und insbesondere der Auffangtatbestand für notwendig gehalten worden. Dies gelte auch für die Eingrenzung, die seitens des Datenschutzbeauftragten auf Seite 9 seines Zusatzberichtes vorgeschlagen werde. Wenn man diesen Vorschlägen folge, sei APIS als Recherchedatei sinnlos. Das Bundeskriminalamt und die Arbeitsgemeinschaft der Leiter der Landeskriminalämter und des Bundeskriminalamts, insbesondere die hier in Betracht kommende Staatsschutzkommission, bemühten sich jedoch, das Kriterium der verfassungsfeindlichen Zielsetzung so genau wie möglich zu fassen. Es würden Indizien erarbeitet, die früheres Verhalten beträfen. Die verfassungsfeindliche Zielsetzung müsse künftig schriftlich begründet werden. Man wolle sich auf der Arbeitsebene besser darüber abstimmen, was z. B. bei einer Tat als verfassungsfeindliche Zielrichtung in Betracht kommen könne und auf die Speicherung von Ordnungswidrigkeiten verzichten. Die Bundesregierung halte diese Bestrebungen für sinnvoll.

Die Fraktion der SPD führte im Rahmen der Beratungen im Innenausschuß zusätzlich zu den in ihrem Beschlußempfehlungsvorschlag enthaltenen Vorbringen aus, der Bereich von APIS sei vom engen Terrorismusbereich her immer mehr ausgeweitet worden und habe die Qualität einer Datei erreicht, die eher dem Verfassungsschutz zuzuordnen sei. Sie habe sich immer mehr in Richtung auf eine Gesinnungsdatei hin entwickelt, was nicht nur auf der Errichtungsanordnung, sondern auch auf der Miteinbeziehung des Extremismusbereichs beruhe. Die rechtliche Zulässigkeit von APIS sei nicht geklärt und problematisch. Diese Frage könne nicht durch den Hinweis auf den Übergangsbonus beantwortet werden. Hinsichtlich der Problematik, daß gestützt auf den Auffangtatbestand in der Errichtungsanordnung überwiegend Kleinkriminalität in APIS gespeichert werde, wies sie darauf hin, daß der Datenschutzbeauftragte in seinem Bericht über die Datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamts in der Zeit vom 1. Dezember 1987 bis zum 29. Januar 1988 auf Seite 9 zu dem Bereich der „anderen Straftaten" vier Kriterien genannt habe. Man schließe sich diesen an, wohl wissend, daß diese nicht ausreichten, um das Grundproblem zu lösen, und empfehle, daß aufgrund dieser vier Punkte eine Einigung zwischen dem Bundesminister des Innern bzw. dem Bundeskriminalamt und dem Datenschutzbeauftragten erreicht werden solle.

Die Fraktion der CDU/CSU wies demgegenüber darauf hin, daß der Datenschutzbeauftragte auf Seite 2 seines zusätzlichen Berichts über die Datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamts feststelle, daß es im Bereich von APIS wesentliche Verbesserungen gegeben habe. Seit 1982 sei der Aktenbestand halbiert worden. In den eingesehenen Fällen habe die Anlegung der Kriminalakten stets auf der Einleitung polizeilicher Ermittlungsverfahren beruht. Man sei der Meinung, daß APIS auf der Grundlage des Übergangsbonus habe errichtet werden dürfen, da der Übergangsbonus auch die Errichtung neuer Dateien gestatte, wenn diese erforderlich seien. In absehbarer Zeit würden gesetzliche Grundlagen in der Strafprozeßordnung und dem Bundeskriminalamtgesetz geschaffen. Der Auffangtatbestand in der Errichtungsanordnung und damit das Überschreiten des reinen Staatsschutzdeliktsbereichs sei notwendig, wenn die Datei einen Sinn haben solle. Eine staatsfeindliche Absicht allein führe nicht zur Speicherung in APIS. Die Aufnahme in die Datei erfolge nur, wenn die kriminelle Tat und die verfassungsfeindliche Zielsetzung erkennbar seien. Man halte das bisherige Verfahren grundsätzlich für vertretbar: Es gelte, Kleinkriminalität, die als Einstiegskriminalität für schwere Delikte erkennbar sei, rechtzeitig zu erfassen. Die Frage sei, ob bei der Anwendung der Richtlinien zu weit gegangen werde. Dies sei jedoch kein Argument, das grundsätzlich gegen das Bestehen eines Auffangtatbestandes spreche. Die Länder müßten ihren Beurteilungsspielraum entsprechend dem Grundsatz der Verhältnismäßigkeit ausüben; ggf. müsse ihr Beurteilungsspielraum eingegrenzt werden.

Seitens der Fraktion der FDP wurde erklärt, problematisch sei das Verhältnis der eigentlich gemeinten Staatsschutzdelikte zu den Auffangtatbeständen. Hier hätten sich zahlenmäßig Sinn und Ausnahme vollkommen verkehrt. Die Auffangtatbestände bildeten die ganz überwiegende Masse der gesamten Speicherungen. Man dürfe die Frage der Speicherung der Kleinkriminalität nicht davon abhängig machen, daß man schematisch annehme, ein Täter könne später einmal Terrorist werden. Eine vermutete innere Absicht sei kein Speicherungskriterium, wenn man nicht zu einer Gesinnungsdatei kommen wolle. Im übrigen sei eine Datenerfassung von Personen, die weder eine Straftat begangen hätten, noch einer Straftat verdächtig seien, rechtlich unzulässig. Daten über Personen, die z. B. von Volkszählungsbögen Nummern abschnitten, zu speichern, weil sie möglicherweise Staatsfeinde werden und Staatsschutzdelikte begehen könnten, die APIS-würdig seien, werde die polizeiliche Arbeit drastisch erschweren. Diese Mentalität entspreche einem Verfassungsschutzdenken und gehöre nicht in den kriminalpolizeilichen Bereich. Die Errichtungsanordnung für APIS müsse präzisiert werden. Wenn dies nicht geschehe, müsse der Gesetzgeber Folgen daraus ziehen.

Die Fraktion DIE GRÜNEN hat in ihrem Beschlußempfehlungsvorschlag (siehe Ziffer 4.2 dieses Berichts) zu dem Thema „Speicherung von Kleinkrimi-

nalität in APIS" Stellung genommen und im Innenausschuß dementsprechend ausgeführt, mit der Begründung, jeder Terrorist habe klein angefangen, würden in der APIS-Datei keine Terroristen gespeichert, sondern die Betroffenen durch die Speicherung zu Terroristen gemacht. Wenn sogenannte Staatsfeinde neben Kleinstkriminellen gespeichert würden, zeige das die undifferenzierten, pauschalen Kriminalisierungsabsichten der Polizeibehörden. Weil Menschen allein wegen ihrer vermuteten staatsfeindlichen Gesinnung anläßlich von Verhalten wie des Aufrufens zum Herausschneiden von Nummern aus dem Volkszählungsbogen, wildem Plakatieren oder des Sprühens eines roten Kreises auf eine Mauer (DER SPIEGEL Nr. 28, 11. Juli 1988) in APIS gespeichert würden und solche Banalitäten 70% des gesamten Dateibestandes ausmachten, sei diese Praxis sofort zu stoppen; alle bisherigen Einspeicherungen seien ohne Ausnahme zu löschen.

4.1.10 Zu Nummer X

Nummer X des Beschlußempfehlungsvorschlags der Fraktion der SPD bezieht sich auf Kapitel 13.3b des Neunten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz sowie auf Seite 46 der Stellungnahme der Bundesregierung hierzu.

Seitens der Bundesregierung wurde im Rahmen der Beratungen im Innenausschuß ergänzend ausgeführt, daß das Bundeskriminalamt — Abteilung Staatsschutz — NADIS als Aktenfundstellensystem für Kriminalakten benutze, die bei dieser Abteilung über Verdächtige und Beschuldigte angelegt würden. Die Voraussetzungen hierfür ergäben sich aus Ziffer 1 der Richtlinien für den kriminalpolizeilichen Meldedienst. Im Rahmen des geltenden Rechts sei es ausreichend, daß das Bundeskriminalamt in der Errichtungsanordnung von NADIS als Verbundteilnehmer genannt sei und auch die KpS-Richtlinien einschlägig seien. NADIS ermögliche dem Bundeskriminalamt eine eigene Aktenverwaltung. Die Abteilung Staatsschutz benötige ein Aktenfundstellensystem. Offen sei, ob das bestehende System gebraucht werde. Die Einspeicherung von NADIS erfolge zusammen mit einer kriminaltaktischen Anfrage. Diese führe noch nicht automatisch beim Bundeskriminalamt zu einer Einspeicherung in APIS. Das Bundesamt für Verfassungsschutz könne diese Informationen auch auf anderem Weg erhalten. Es erfahre durch die Verbunddatei nur die Fundstelle. Die Akten würden auf anderem Wege übersandt. Das Bundesamt für Verfassungsschutz habe ein legitimes Interesse daran zu erfahren, ob beim Bundeskriminalamt Erkenntnisse über Straftaten vorlägen, die extremistisch motiviert seien. Rechtlich sei nicht zu beanstanden, daß eine Sicherheitsbehörde bei einer anderen anfrage, um relevante Informationen zu erhalten. Die Frage des unmittelbaren Zugriffs sei notwendigerweise in Zusammenhang damit zu sehen, daß in NADIS lediglich Aktenzeichen gespeichert würden. Die Relevanz einer Information werde beim Bundesamt für Verfassungsschutz im Rahmen der Erstbehandlung überprüft. Ein Rückzug des Bundeskriminalamts aus NADIS setze die Klärung der Frage voraus, auf welche sonstige Weise das berechtigte Informationsinteresse des Verfassungsschutzes in bezug auf polizeiliche Staatsschutzerkenntnisse sichergestellt werden könne; diese Frage sei im Zusammenhang mit der Novellierung des Bundesverfassungsschutzgesetzes zu sehen. In § 4 Abs. 2 des Entwurfs des Verfassungsschutzgesetzes sei vorgesehen, die gemeinsamen Dateien der Verfassungsschutzbehörden als exklusive Verfassungsschutzdateien zu führen, mit der Folge, daß ein nicht diesem inneren Kreis angehöriger Behördenbereich zu den Verbunddateien keinen Zugang hätte. Dies habe auf den gegenwärtigen Zustand jedoch keine unmittelbare Auswirkung.

Seitens des Bundesbeauftragten für den Datenschutz wurde darauf hingewiesen, daß es um einen gegenwärtig vorliegenden Rechtsverstoß gehe, der darin liege, daß das Bundeskriminalamt derzeit Fundstellen von Akten aus seiner Abteilung Staatsschutz im nachrichtendienstlichen Informationssystem NADIS einstelle und damit den anderen NADIS-Teilnehmern direkten Zugriff auf diese Fundstellen ermögliche. Das Problem liege in der Frage, was in NADIS eingespeichert werden dürfe, und wer dies derzeit benutzen dürfe. Über die Frage der Einspeicherung in NADIS müsse grundsätzlich das Bundesamt für Verfassungsschutz entscheiden. Deswegen seien dort die Verkartungspläne angelegt. Derzeit würden Daten, selbst wenn sie für das Bundesamt für Verfassungsschutz erklärtermaßen nicht relevant seien, in NADIS gespeichert. Er sei sicher, daß bei einem großen Teil der NADIS-Einspeicherungen die gesetzlichen Voraussetzungen nicht vorlägen, da über die Datei APIS hinaus, die schon weit formuliert sei und die verfassungsfeindliche Zielsetzung impliziere, Einspeicherungen in NADIS vorgenommen würden.

Die Fraktion der SPD wies im Rahmen der Beratungen im Innenausschuß darauf hin, daß der Bundesbeauftragte für den Datenschutz in seinem Sonderprüfbericht über die Datenschutzrechtliche Kontrolle bei der Abteilung Staatsschutz des Bundeskriminalamtes zum einen die Frage der fehlenden Errichtungsanordnung für NADIS-PZD angesprochen habe sowie die Tatsache, daß in NADIS-PZD teilweise mehr als doppelt so viele Speicherungen vorgenommen worden seien wie in APIS. Die Fraktion der SPD habe bereits bemängelt, daß die Kriterien für Speicherungen in APIS völlig unzureichend seien und stelle jetzt fest, daß bei NADIS noch weitere Spielräume vorhanden seien. In Zusammenhang mit der Volkszählung seien über 71 Personen bestehende Kriminalakten ergänzt und 89 neue Kriminalakten angelegt worden. Angesichts der nicht vorhandenen Errichtungsanordnung reiche der Hinweis auf die KpS-Richtlinien nicht aus. Hinsichtlich der Übermittlung von Daten aus NADIS an Verfassungsschutzbehörden sei das derzeitige Verfahren nicht haltbar. Der Nachrichtenaustausch mit den Verfassungsschutzbehörden sei nicht geringer als der polizeiinterne Nachrichtenaustausch. Dies sei nicht vertretbar. Man stimme der seitens des Bundesbeauftragten für den Datenschutz in seinem erneuten Bericht aufgestellten Empfehlung zu: Sofortmaßnahme bis zur Löschung der BKA-Datensätze und Fundstellen in NADIS-PZD solle die Beendigung des Zugriffs der übrigen NADIS-Teilnehmer auf diese

Speicherungen sein. Seitens der Fraktion der SPD werde die Einstellung der Datei gefordert.

Die Koalitionsfraktionen betonten, daß es sich bei NADIS lediglich um eine Aktennachweisdatei handele, die keine darüber hinausgehenden Daten enthalte. Man sei sich in den Berichterstattergesprächen darüber einig gewesen, daß der Datenverbund von Bundeskriminalamt und Verfassungsschutz über NADIS, seitdem APIS existiere, nicht im Interesse des Bundeskriminalamtes, sondern nur für das Verfassungsschutzamt erforderlich sei, damit ihm die Kenntnis über die den Staatsschutz betreffenden Daten vermittelt würde, die das Bundeskriminalamt und die entsprechenden Landesbehörden hätten. Man sei sich auch darüber einig gewesen, daß eine gesetzliche Grundlage hierfür nötig sei. Nach den Gesetzentwürfen der Bundesregierung sei die gemeinsame Benutzung einer einzigen Datei durch Verfassungsschutz und Bundeskriminalamt rechtlich nicht mehr zulässig.

Die Fraktion DIE GRÜNEN hat im Rahmen der Beratungen im Innenausschuß bemängelt, daß das, was man an APIS kritisiere, in NADIS fortgesetzt und sogar noch ausgeweitet werde. Man unterstütze die Vorschläge des Bundesdatenschutzbeauftragten für den Datenschutz zu dieser Thematik. Die nach dem Krieg von den Alliierten verfügte Trennung von Nachrichtendiensten und exekutiver Polizei werde völlig unterlaufen. Schon insoweit sei Unzulässigkeit gegeben. Die Fraktion DIE GRÜNEN hat zudem einen eigenen Beschlußempfehlungsvorschlag zu dieser Thematik eingebracht (siehe Ziffer 4.2 dieses Berichts).

4.1.11 Nummer XII

Die Fraktion DIE GRÜNEN hat sich dem Wunsch auf Abgabe eines Gesamtberichts über den Einsatz von Personalcomputern in den Bundesverwaltungen ausdrücklich angeschlossen. Die Bundesregierung erklärte, der gewünschte Bericht werde voraussichtlich im Laufe des Jahres 1989 vorgelegt werden.

4.2 Beschlußempfehlungsvorschlag der Fraktion DIE GRÜNEN

Die Fraktion DIE GRÜNEN hat eigene Beschlußempfehlungsvorschläge eingebracht, die im Innenausschuß mehrheitlich mit den Stimmen der Koalitionsfraktionen bei Enthaltung der Fraktion der SPD abgelehnt wurden.

Die Beschlußempfehlungsvorschläge der Fraktion DIE GRÜNEN einschließlich der von der Fraktion beigefügten schriftlichen Begründungen haben folgenden Wortlaut:

„— Ausländerzentralregister

Der Innenausschuß möge beschließen:

Die Bundesregierung wird aufgefordert, die Speicherung von ausländischen Mitbürgern/innen im Ausländerzentralregister einzustellen, das gesamte Register zu löschen und auf jegliche Datenerhebung und Speicherung der ausländischen Mitbürger/innen in Zukunft zu verzichten.

Begründung

Die Erfassung und Kontrolle von Personengruppen, insbesondere gesellschaftlichen Minderheiten, wird grundsätzlich abgelehnt.

— Automatisierte Personaldatenverarbeitung

(Kapitel 5.2 in Drucksache 10/4690 und Kapitel 7.2 in Drucksache 10/6816)

Die Bundesregierung wird aufgefordert, unverzüglich den Entwurf einer bereichsspezifischen Regelung des Arbeitnehmer/innen-Datenschutzes vorzulegen, wie sie es u. a. in ihrer Stellungnahme zum Achten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz angekündigt hat.

Dieser Entwurf muß folgende Regelungen enthalten:

1. Die Beschränkung der Datenerhebung, -speicherung, -verwertung und -übermittlung auf einen genau festgelegten Zweck; dies umfaßt auch die Beschränkung des Fragerechts des Arbeitgebers sowie der Einstellungsuntersuchungen und Persönlichkeitstests;
2. das Verbot der automatischen Verarbeitung dienst- und arbeitsrechtlicher Beurteilungsnoten der/des Beschäftigten;
3. das Verbot der automatischen Verarbeitung medizinischer und psychologischer Befunde oder von Daten, aus denen diese abgeleitet werden können;
4. das Verbot jeglicher Verhaltens- und Leistungskontrolle mittels technischer Systeme;
5. das Verbot der Speicherung der Zielnummer bei der Benutzung dienstlicher Telefonnebenstellenanlagen sowie die strikte Zweckbindung bei der Verarbeitung von Gebührendaten;
6. das Verbot des Abgleiches von personenbezogenen Daten, die zu verschiedenen Zwecken erhoben wurden, und die Verpflichtung zur Schaffung von technischen Vorkehrungen zur Sicherung dieses Verbotes, insbesondere die Speicherung der Daten auf getrennten Rechnersystemen auf Verlangen der betrieblichen Interessenvertretung der Betroffenen;
7. das Verbot von Auswertungen und Verknüpfungen, die zur Herstellung eines „Persönlichkeitsabbildes" der Arbeitnehmer/innen führen können;
8. die Pflicht des Arbeitgebers zur kostenlosen Auskunft aller über den/die Arbeitnehmer/in gespeicherten personenbezogenen Daten unter Angabe des Zweckes der Speicherung, der Herkunft der

Daten und Mitteilungen der Stellen, an welche die Daten weitergegeben wurden;

9. die Pflicht zur Lösung

   a) unrichtiger Daten und solcher, deren Richtigkeit vom Betroffenen bestritten wird, wenn der Arbeitgeber nicht innerhalb eines angemessenen Zeitraumes die Richtigkeit beweist;

   b) der Daten, deren Speicherung für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, mit Festlegung eines Zeitraumes, nach dessen Ablauf die Daten spätestens zu löschen sind, wenn nicht Rechtsvorschriften oder die ausdrückliche Einwilligung des Betroffenen eine längere Speicherung erlauben;

10. die Schaffung eines verschuldensunabhängigen Schadensersatzanspruches für materielle und immaterielle Schäden, die bei der — konventionellen und elektronischen — Datenverarbeitung von Arbeitnehmer/innen-Daten entstehen, wobei dem Arbeitgeber auch Schäden zugerechnet werden müssen, die von einer anderen Stelle, an die der Arbeitgeber die Daten weitergegeben hat, verursacht werden;

11. — Mitbestimmungsrecht der Arbeitnehmer/innen-Vertretung bei der Bestellung und Abberufung des/der betrieblichen Datenschutzbeauftragten;

    — Verankerung seiner/ihrer Unabhängigkeit vom Arbeitgeber im Gesetz;

    — Schaffung einer gesetzlichen Pflicht zur Zusammenarbeit von Datenschutzbeauftragter/-beauftragtem und Betriebsrat;

    — Beratungsrecht der Arbeitnehmer/innen-Vertretung und der/des Datenschutzbeauftragten bei der Auswahl der in der betrieblichen Datenverarbeitung tätigen Personen;

12. gesetzliche Verankerung der Pflicht des Arbeitgebers, der/dem Datenschutzbeauftragten des Betriebes auf Verlangen alle für die Erfüllung ihrer/seiner Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen;

13. Verschwiegenheitspflicht der/des betrieblichen Datenschutzbeauftragten gegenüber dem Arbeitgeber bezüglich der beim Betriebsrat vorhandenen Daten;

14. gesetzliche Verankerung eines besonderen Kündigungsschutzes entsprechend § 15 Kündigungsschutzgesetz für die/den Datenschutzbeauftragte/n und Verbot von Interessenkollision zu ihrer/seiner sonstigen Tätigkeit im Betrieb;

15. Vetorecht und Sicherung der betrieblichen Interessenvertretung bei der durch Datenfernübertragung ermöglichten Auslagerung von Arbeitsplätzen und Schaffung sogenannter Teleheimarbeitsplätze;

16. Mitbestimmungsrecht der Arbeitnehmer/innen-Vertretung bei Planung, Einführung und Ausbau aller Systeme für die automatisierte Personaldatenverarbeitung (Personalinformationssysteme) des Betriebes;

17. Pflicht der Aufsichtsbehörde, die/den Betroffene/n im Falle des Verdachtes einer strafbaren Handlung nach § 41 Bundesdatenschutzgesetz auf ihr/sein Antragsrecht hinzuweisen;

18. soweit die gewerberechtlichen Auflagen den Datenschutz betreffen, sind diese der Datenschutzaufsichtsbehörde (§ 30 Bundesdatenschutzgesetz) zu übertragen;

19. Erweiterung der Rechte und Pflichten der Aufsichtsbehörden zum Schutz der betroffenen Arbeitnehmer/innen dahin, daß über die Aufsichtspflicht hinaus der Aufsichtsbehörde ein eigenständiges Kontrollrecht eingeräumt wird und sichergestellt wird, daß die Aufsichtsbehörde nach § 30 Bundesdatenschutzgesetz für die Verfolgung und Ahndung der Ordnungswidrigkeiten zuständig ist.

— Post- und Fernmeldewesen

Der Innenausschuß möge beschließen:

Die Bundesregierung wird aufgefordert,

— darauf hinzuwirken, daß der Postminister alle Planungen unverzüglich dem Bundesbeauftragten für den Datenschutz zur Beratung vorlegt, dessen Kritik in praktische Datenschutz-Vorkehrungen umsetzt und die Zusammenarbeit mit dem BfD nicht erschwert oder behindert;

— die Weitergabe der Anschriften von Postkunden an die Deutsche Postreklame zu verbieten;

— die Zwangseintragung der Teilnehmer/innen am öffentlichen Fernsprechnetz in das Telefonbuch zu verbieten;

— die Übermittlung der Anschriften von z. B. Neugeborenen und Konfirmanden zu Werbezwecken durch Postzusteller/innen zu untersagen;

— den direkten Zugang des BfD zu den Personalvertretungen der Postbehörden zu gewährleisten;

— die Speicherung von Telefonverbindungsdaten zu verbieten.

— Telekommunikationsordnung

Der Innenausschuß möge beschließen:

Die Bundesregierung wird aufgefordert, nicht hinter den Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zurückzufallen:

„Deshalb muß z. B. selbstverständlich sein, daß alle personenbezogenen Daten aus der Bild-, Sprach-, Text- und Datenübertragung geschützt werden." „Die Regelung der Zulässigkeit der Verarbeitung personenbezogener Daten, deren Kontrollen und der erforderlichen technisch-organisatorischen Maßnahmen müssen an die neuen technischen Gegebenheiten angepaßt werden."

Da auch die bisher bekanntgewordenen Entwürfe der Novellierung des BDSG mit ihren allgemeinen Vorschriften die Risiken der Telekommunikation nicht auffangen können, bedarf es weiterer spezieller Regelungen.

— Deutsche Bundesbahn — Videoaufzeichnungen

Der Innenausschuß möge beschließen:

Die Bundesregierung wird aufgefordert, jegliche Videoaufzeichnungen auf Bahnhöfen zu verbieten.

Jede Bildaufzeichnung verstößt gegen das Persönlichkeitsrecht der Bahnkunden. Diese Speicherungen — die nicht einmal der Kontrolle des Bundesbeauftragten für den Datenschutz unterliegen — werden ohne Einwilligung der Betroffenen vorgenommen.

Auch eine kurzfristige Speicherung verstößt gegen das informationelle Selbstbestimmungsrecht. Längerfristige Aufzeichnungen der Daten führen zu einer unzumutbaren Beobachtung der Betroffenen, aus denen sogenannte Bewegungsbilder erstellt werden können.

— Verteidigung — Eignungs- und Verwendungsprüfung (9. Bericht des BfD 18.3)

Der Innenausschuß möge beschließen:

Die Bundesregierung wird aufgefordert, keine computergestützten Eignungstests bei Wehrpflichtigen zuzulassen.

Darüber hinaus wird die Bundesregierung aufgefordert, eine Novellierung des § 20a Wehrpflichtgesetz vorzunehmen, in der präzise bestimmt wird, was vom Wehrpflichtigen für die EVP verlangt wird, welche Folgen das Ergebnis der Fragen für ihn hat und rechtliche Absicherungen, d. h. Geheimhaltungspflicht des Psychologischen Dienstes.

Begründung

Der BfD führt im Neunten Tätigkeitsbericht aus:

„Außer den bloßen Testergebnissen können bei computergestützten Tests noch andere personenbezogene Daten gewonnen werden, die ebenfalls Aussagen über die Leistungsfähigkeit und die Eignung ermöglichen."

Diese Erfassung von zusätzlichen Merkmalen und Daten der Wehrpflichtigen verstößt gegen das Volkszählungsurteil von 1983.

— Datenübermittlung von Bundesbehörden an ausländische Dienststellen oder private Empfänger

Bundesbehörden übermitteln Informationen über Bewohner/innen der Bundesrepublik Deutschland nur dann an ausländische Empfänger, wenn nachprüfbar sichergestellt ist, daß deren weitere Verarbeitung dieser Daten bundesdeutschen Datenschutz-Standards genügt.

Begründung

Der Verfassungsgrundsatz der Zweckbindung darf nicht jenseits der Grenze enden. Das Grundrecht auf informationelle Selbstbestimmung muß vielmehr durch deutsche Behörden bei Datenübermittlungen an ausländische Empfänger durch die empfohlene Beschränkung geschützt werden.

Wie aktuell diese Maßnahme ist, zeigen die Entwicklungen anläßlich der geplanten Aufhebung der europäischen Binnengrenzen und z. B. der zwischen den Schengener Vertragsstaaten beabsichtigte Betrieb eines gemeinsamen Informationssystems, welches keine Einschränkungen des bundesdeutschen Datenschutz-Standards mit sich bringen darf.

— NADIS-Verbund

1. Der Zugang des Berliner Landesamtes für Verfassungsschutz zu NADIS wird gekappt. Die Bundesregierung wird aufgefordert, sich umgehend unter den anderen NADIS-Teilnehmern/Bundesländern für eine dahin gehenden Änderung der Verbund-Vereinbarungen einzusetzen.

2. Konventionelle Anfragen des Berliner Landesamtes für Verfassungsschutz werden durch Bundesbehörden ab sofort nicht mehr beantwortet.

Begründung

Nach den Enthüllungen der letzten Zeit über die oft rechtswidrigen Praktiken des Berliner Landesamts für Verfassungsschutz sowie über deren Zusammenarbeit mit Dienststellen der Drei Mächte dabei, welche offenbar häufig „auf dem kurzen Dienstweg" und unter Mißachtung deutscher Datenschutz-, insbesondere Übermittlungs-Regelungen geschieht, muß befürchtet werden, daß ein „Berliner Loch im Datenschutz" besteht. Eine solche Situation führt jegliche Diskussion über — veränderte und detaillierte — Vorschriften über den Datenverkehr mit ausländischen Dienststellen ad absurdum.

Daraus ist die Konsequenz zu ziehen, daß der online-Zugriff des Berliner LfV (und über dieses auch von Dienststellen der Drei Mächte) auf dem gemeinsamen NADIS-Bestand unterbunden werden muß.

Da auch hinsichtlich konventionell an das Berliner LfV übermittelter personenbezogener Informationen befürchtet werden muß, daß diese über Berliner Dienststellen der Drei Mächte an unkontrollierbar viele weitere Empfänger gelangen, dürfen zumindest Bundesbehörden keine derart gefährdeten Informationen an das Berliner LfV gelangen lassen.

— BKA/APIS

Die Teilnahme des BKA an der Verbunddatei APIS wird umgehend einseitig gekündigt. Alle vom BKA in APIS eingegebenen Daten werden gelöscht und keine weiteren Daten eingegeben.

Begründung

Die Arbeitsdatei PIOS Innere Sicherheit, eingerichtet zur Aufklärung von Staatsschutz- und Terrordelikten, tat sich bisher nicht dadurch hervor, daß sie zur Aufklärung von Straftaten beigetragen hätte, sondern durch Skandale und Verstöße gegen den Datenschutz. Die Speicherung von Umweltschützern, Friedensdemonstranten und Volkszählungsgegnern schlug zu Recht hohe Wellen. Die Speicherung von hochrangigen Politikern, hohen Beamten und Vertretern der Wirtschaft als Kontaktpersonen von „Terroristen" demonstriert deren Absurdität.

Die Datei APIS der Staatsschutzabteilungen der Polizei entspricht in vieler Hinsicht nicht den verfassungsrechtlichen Anforderungen:

— Die Registrierung von politischen Aktivitäten, weitgehend ohne förmliche Feststellung einer strafbaren Handlung, widerspricht der vom Verfassungsgericht geforderten grundsätzlichen Staatsferne demokratischer Willensbildung und der strafrechtlichen Unschuldsvermutung (vgl. BVerfGE 65, 1 ff., BVerfGE 69, 315 ff.).

— Die beliebige Verknüpfbarkeit von Personen, Institutionen, Objekten, Sachen und Ereignissen ermöglicht politische Sozialprofile und stellt einen unverhältnismäßigen Eingriff in Grundrechte dar.

— Die Einbeziehung aller irgendwie aus Polizeisicht politisch motivierten Straftatverdächte über die Kategorie der „anderen Straftaten" bis hinein in den Bagatellbereich verstößt gegen das Grundrecht auf informationelle Selbstbestimmung und widerspricht dem verfassungsmäßigen Bestimmtheitsgebot und dem Verhältnismäßigkeitsprinzip.

— Das Betreiben einer redundanzfreien Polizei-Verbunddatei auf Bundesebene widerspricht dem föderalen Prinzip und der ausschließlichen Landeszuständigkeit in Polizeisachen, da die durch einzelne Länder angelieferten Daten nicht eigenständig verwaltet werden.

— APIS wurde am 2. Januar 1986 in Betrieb genommen, ohne daß eine gesetzliche, verfassungsmäßig geforderte Grundlage bestünde.

— Die Einbeziehung „anderer Personen" und „Gefährdeter" und deren potentielle minutiöse Personenbeschreibung verletzt den Verhältnismäßigkeitsgrundsatz.

— Datenschutz und Datenrichtigkeit sind organisatorisch nicht gewährleistet, z. B. wegen Fehlens von Nachberichtspflichten und wegen unvollständiger Auskunftserteilung gegenüber den betroffenen Bürgern/innen.

— Durch die Übermittlung von APIS-Daten an andere Stellen, insbesondere die Geheimdienste, wird das Zweckbindungsprinzip und die verfassungsrechtlich geforderte Trennung von Polizei und Geheimdiensten verletzt.

Auf diese Verfassungsverstöße wurde von seiten fast aller Datenschutzbeauftragten in der Bundesrepublik Deutschland immer wieder hingewiesen, ohne daß dies Konsequenzen gezeigt hätte (Bundesbeauftragter für den Datenschutz: BT-Drucksache 9/2386 Seite 89, BT-Drucksache 10/877 Seite 46, BT-Drucksache 10/2777 Seite 68, BT-Drucksache 10/6816 Seite 61 ff., BT-Drucksache 11/1693 Seite 77 f., BT-Drucksache 11/3932 Seite 63 ff.; Datenschutzkommission Rheinland-Pfalz: rhpfLT-Drucksache 11/710; Landesbeauftragte für den Datenschutz bawüLT-Drucksache 9/5230 Seite 51 ff., bawüLT-Drucksache 10/950 Seite 19 ff., bayLT-Drucksache 10/8252 Seite 29, bayLT-Drucksache 11/60 Seite 27, berl-AbgH-Drucksache 10/1883 Seite 10, 10. JBbremLfD 1988 Seite 46 f., 6. TBhambgLfD 1987 Seite 82 ff., 11. TbhessLfD 1982 Seite 72 f., 16. hessLfD 1987 Seite 147 f., saarl. LT-Drucksache 9/1521 Seite 50 f., shLT-Drucksache 12/10 Seite 28).

Um diesen verfassungswidrigen Zustand zumindest für die Bundespolizeibehörde BKA zu beenden, bedarf es der geforderten Maßnahme.'

In bezug auf diejenigen Themen, die in der Beschlußempfehlung und im Alternativantrag der Fraktion der SPD aufgegriffen wurden, ist hinsichtlich der Beratungsergebnisse auf die obigen Ausführungen zu Ziffern 3 und 4.1 zu verweisen. Von den übrigen im Antrag der Fraktion DIE GRÜNEN angesprochenen Fragenbereichen wurden die im folgenden aufgeführten näher erörtert:

— Zum Bereich „automatisierte Personalaktenverarbeitung, Personalinformationssysteme" (Kapitel 7.2 des Neunten Tätigkeitsberichts):

  Die Fraktion der SPD wünschte eine Stellungnahme des Datenschutzbeauftragten zur Personaldatenverarbeitung im Deutschen Patentamt.

  Der Bundesbeauftragte für den Datenschutz legte dar, man habe im vergangenen Jahr eine Nachkontrolle beim Deutschen Patentamt durchgeführt. Ausführungen hierzu fänden sich im Elften Tätigkeitsbericht. Es habe sich zwar einiges gebessert, ganz zufrieden sei man jedoch noch nicht. Die Situation des dortigen internen Datenschutzbeauftragten sei inzwischen befriedigend gelöst.

— Zum Bereich Post- und Fernmeldewesen (Kapitel 8 des Neunten Tätigkeitsberichts):

  Die Fraktion der SPD wünschte im Innenausschuß nähere Auskünfte hinsichtlich des Bereichs der Telefondatenverarbeitung, insbesondere hinsichtlich der Problematik einer Speicherung der Zielnummer.

  Der Bundesbeauftragte für den Datenschutz legte dar, es gebe in diesem Bereich den Entwurf einer

Regelung, die demnächst in Kraft treten solle. Mit dieser könne der Bundesbeauftragte für den Datenschutz zufrieden sein. Der Bundesbeauftragte für den Datenschutz führte im übrigen hinsichtlich der Beschlußempfehlungsvorschläge der Fraktion DIE GRÜNEN zu den Themen „Automatisierte Personaldatenverarbeitung", „Telekommunikationsordnung", „Post- und Fernmeldewesen" aus, die Kooperation mit dem Bundesminister für das Post- und Fernmeldewesen habe sich erfreulich entwickelt. Man treffe sich in ¼jährlichen Abständen zwecks Erörterung der anstehenden Dinge.

— Zum Bereich Deutsche Bundesbahn — Videoaufzeichnungen:

Der Bundesbeauftragte für den Datenschutz übt unter Punkt 7.3 seines Achten und unter Punkt 9.6.2 seines Neunten Tätigkeitsberichts Kritik an Video-Überwachungen durch die Deutsche Bundesbahn.

Die Bundesregierung schilderte die Fälle, in denen Videoaufzeichnungen stattfänden. Wenn z. B. bei der Frachtbeförderung oder in Gepäckabteilungen Diebstähle vorkämen und man ganz konkreten Fällen nachgehe, führe man Fahndungen auch unter Zuhilfenahme von Videoaufzeichnungen durch. Der Bundesbeauftragte für den Datenschutz habe bestätigt, daß es sich um Einzelfälle handele, in denen Aufzeichnungen, die nicht mehr benötigt würden, in angemessener Zeit gelöscht würden. Ein zweiter Fall betreffe Betriebsstörungen an Halbschranken. Die Bundesbahn habe zur Aufklärung der Ursachen der Störungen zum Teil Videobeobachter eingesetzt und teilweise Aufzeichnungen angefertigt. Passanten seien hierin jedoch nicht zu erkennen. Hierbei gehe es um die Frage, ob es sich um betriebliche Überwachungssysteme i. S. der Betriebsverfassung handele und daher der Personalrat beteiligt werden müsse. Diese Frage werde kritisch geprüft. Im Bereich der Hamburger S-Bahn werde, weil Personalknappheit bestehe, jedoch die Betriebssicherheit gewährleistet sein solle, automatisch bei Abfahrt eines jeden Zuges für 10 Sekunden eine Aufzeichnung gemacht, auf der man sehen könne, in welchem Zeitpunkt Personen in die S-Bahn einstiegen. Diese Aufzeichnungen würden ggf. durch konkreten Eingriff verlängert, wenn sich ein Unfall ereigne. Dies diene der Beweissicherung für die Aufklärung von Unfällen. Es werde von den Aufzeichnungen nur im Falle eines Unfalls Gebrauch gemacht, wenn man der Frage weiter nachgehen müsse, ob Haftungspflichten bestünden. Man könne bei diesen Aufzeichnungen Personen erkennen. Wenn sich kein Unfall ereigne, würden die Aufzeichnungen umgehend durch die jeweils nächste Aufzeichnung wieder gelöscht. Es gebe im Bereich der Deutschen Bundesbahn Monitorüberwachung ohne Aufzeichnung, z. B. zum Zweck der Überwachung der Flächen vor den Schließfächern in Bahnhöfen oder an sonstigen Stellen, an denen die Gefahr von Straftaten oder ordnungsstörenden Handlungen bestehe. Man erleichtere sich hier die Wahrnehmung des Hausrechts der Bundesbahn dadurch, daß man über Monitore von zentralen Stellen aus Beobachtungen durchführe. Hier erfolgten jedoch keine Aufzeichnungen.

Die Fraktion DIE GRÜNEN betonte, Videoüberwachungen gewährleisteten nicht den Schutz reisender Personen und seien generell abzuschaffen. Moniert würde ebenfalls die zunehmende Videoüberwachung in Kaufhäusern.

Die Fraktion der SPD betonte demgegenüber, Videoaufzeichnungen könnten durchaus sowohl für den Bürger als auch für die Institution, für die sie erhoben worden seien, sinnvoll sein. Es müßten jedoch entsprechend kurze Löschungsfristen festgelegt sein. Die gleiche Problematik betreffe auch Bankgebäude und viele öffentliche Gebäude.

5. Weitere Beratungsschwerpunkte

5.1 Voten mitberatender Ausschüsse

Soweit einzelne Voten ganz oder teilweise bereits unter Ziffern 3.1, 3.2, 3.3 und 4.1.5 einbezogen wurden, wird hierauf verwiesen.

Die Koalitionsfraktionen erklärten, das Votum des Ausschusses für das Post- und Fernmeldewesen, des Ausschusses für Arbeit und Sozialordnung und des Ausschusses für Jugend, Familie, Frauen und Gesundheit werde jeweils in vollem Umfang mitgetragen.

Die Fraktion der SPD sprach sich dafür aus, daß der Innenausschuß die einstimmig beschlossenen Empfehlungen der mitberatenden Ausschüsse insgesamt übernehmen solle.

5.2 Aufnahme personenbezogener Daten in Berichte des Bundesamtes für Verfassungsschutz über Großereignisse

Der Bundesbeauftragte für den Datenschutz spricht diese Problematik auf Seite 11 des Teils seines Neunten Tätigkeitsberichts an, der als Verschlußsache eingestuft ist.

Nach längerer Diskussion stimmten die Bundesregierung, der Bundesbeauftragte für den Datenschutz, die Koalitionsfraktionen sowie die Fraktion der SPD folgender Lösung zu:

Auf die Aufnahme personenbezogener Daten bei Lageberichten ist grundsätzlich zu verzichten — Ausnahme: bei Personen der Zeitgeschichte —, es sei denn, daß im Einzelfall eine andere Regelung erforderlich ist.

Bei der Novellierung der Dienstvorschrift des Bundesamtes für Verfassungsschutz für die Auswertung soll unter Nummer 17 die Notwendigkeit einer Erforderlichkeitsprüfung aufgenommen werden. Sowohl die Erforderlichkeit als auch die Wahrung schutzwürdiger Belange des Betroffenen sollen dabei als Kriterien hervorgehoben werden. Eine Prüfung der Erforderlichkeit soll sowohl bei der Abfassung der Berichte als auch im Bereich der Übermittlung der personenbezogenen Daten erfolgen.

Die Koalitionsfraktionen betonten, es könne unter Berücksichtigung dieses Lösungsvorschlags von einer willkürlichen Speicherung keine Rede sein und dürfe nur in Ausnahmefällen eine Speicherung erfolgen.

Die Fraktion DIE GRÜNEN kritisierte, daß durch die Erfassung und Speicherung personenbezogener Daten bei Großereignissen durch den Verfassungsschutz das Versammlungsrecht gefährdet und ausgehöhlt werde. Es solle eine genaue Ausformulierung hinsichtlich der Erforderlichkeitsprüfung vorgelegt werden, wobei neben Kriterien auch Beispiele aufgeführt sein müßten.

Mit Schreiben vom 17. Januar 1989 teilte die Bundesregierung mit, der Forderung des Bundesbeauftragten für den Datenschutz, bei Berichten des Bundesamtes für Verfassungsschutz über Großereignisse, die inländischen und ausländischen Stellen zugeleitet würden, abgesehen von Personen der Zeitgeschichte, möglichst keine personenbezogenen Daten zu übermitteln, sei inzwischen durch eine Änderung der Dienstvorschrift Auswertung des Bundesamtes für Verfassungsschutz Rechnung getragen worden. Nach Nummer 17 Abs. 2 der Neufassung der Dienstvorschrift Auswertung dürften Berichte des Bundesamtes für Verfassungsschutz, die unverändert sowohl inländischen Behörden als auch ausländischen Partnerdiensten zur Verfügung gestellt würden, personenbezogene Daten nur enthalten, soweit die Übermittlung dieser Daten für die Aufgabenerfüllung des Bundesamtes für Verfassungsschutz oder den Empfänger erforderlich sei und schutzwürdige Interessen des Betroffenen nicht überwögen. Für die Anwendung dieser Vorschrift in der Praxis werde durch eine Fußnote klargestellt, daß die Schutzwürdigkeit im allgemeinen zu verneinen sein werde, wenn die betreffende Information z. B. durch Presseveröffentlichungen jedermann zugänglich sei.

5.3 *Abteilung V des Bundesamtes für Verfassungsschutz*

Der Innenausschuß hat sich mit den Ausführungen befaßt, die der Bundesbeauftragte für den Datenschutz auf Seiten 5 bis 10 des Teils seines Neunten Tätigkeitsberichts macht, der als Verschlußsache eingestuft ist, sowie mit seinen ergänzenden Ausführungen in dem gesonderten Prüfbericht über Abteilung V des Bundesamtes für Verfassungsschutz.

Im Laufe der Beratungen wurde seitens des Bundesbeauftragten für den Datenschutz und der Bundesregierung übereinstimmend erklärt, daß die Einzelbeanstandungen des Bundesbeauftragten für den Datenschutz mit wenigen Ausnahmen als berechtigt anerkannt und die entsprechenden Löschungen bzw. Korrekturen in der Personenüberprüfungsdatei (PUD) vorgenommen worden seien. Außerdem sei eine Überarbeitung des Entwurfs einer Errichtungsanordnung für die PUD und der Verzicht auf einige der bisher dort gespeicherten Merkmale angekündigt worden. Darüber hinaus habe der Bundesminister des Innern die Prüfung von zusätzlichen Datensicherungsmaßnahmen sowie eine Reihe weiterer Verbesserungen in Aussicht gestellt.

Mit Schreiben vom 3. Februar 1988 habe der Bundesminister des Innern dem Bundesbeauftragten für den Datenschutz das neue Konzept für die Speicherung von Daten beim Bundesamt für Verfassungsschutz im Zusammenhang mit Sicherheitsüberprüfungen mitgeteilt. Es berücksichtige sowohl die Kritik des Bundesbeauftragten für den Datenschutz an der bisherigen Datenverarbeitung bei der Abteilung V des Bundesamtes für Verfassungsschutz als auch die Konsequenzen aus dem Inkrafttreten der neuen Sicherheitsrichtlinien am 1. Mai 1988. Über dieses Konzept hätten Gespräche zwischen dem Bundesminister des Innern, dem Bundesamt für Verfassungsschutz und dem Bundesbeauftragten für den Datenschutz stattgefunden, die dessen weiterer Konkretisierung gedient hätten. Auf der Grundlage dieser Gespräche sei der Entwurf für die Errichtungsanordnung überarbeitet worden. Diese sei nunmehr durch den Bundesminister des Innern genehmigt worden, nachdem auch der Bundesbeauftragte für den Datenschutz keine Einwände mehr erhoben habe. Mit dem Inkrafttreten der neuen Sicherheitsrichtlinien werde auch die neue Errichtungsanordnung wirksam werden.

Mit der Realisierung der Neukonzeption der PUD würden folgende datenschutzrechtlichen Verbesserungen wirksam werden:

- Es werde in Zukunft nur noch einen Datensatz pro Person und nicht wie bisher verschiedene Datensätze mit zum Teil unterschiedlichem, auch gegensätzlichem Inhalt geben.

- Die gespeicherten Merkmale würden korrigiert, sofern sich bei der laufenden Sachbearbeitung oder bei Wiederholungsüberprüfungen ihre Unrichtigkeit herausstelle. Bisher sei entweder bei der Wiederholungsüberprüfung ein neuer, ggf. abweichender Datensatz gespeichert worden, oder es sei lediglich der Hinweis 160 („sicherheitsrelevante Erkenntnisse nach Abschluß der Sicherheitsüberprüfung") hinzugespeichert worden, ohne daß das jeweils belastende Merkmal korrigiert worden sei.

- Alle vom Bundesbeauftragten für den Datenschutz in seinem Prüfbericht über die Kontrolle bei der Abteilung V wegen Verletzung der besonders geschützten Intimsphäre beanstandeten Merkmale seien gestrichen worden.

- Der Katalog der übrigen Merkmale sei in erheblichem Umfang reduziert worden. Die verbliebenen Merkmale orientierten sich an den Angaben im Rahmen der Sicherheitserklärung nach den neuen, ab 1. Mai 1988 gültigen Sicherheitsrichtlinien.

- Belastende Merkmale würden nur noch gespeichert, wenn sie so relevant seien, daß sie Eingang in den Abschlußbericht an den Geheimschutzbeauftragten gefunden hätten. Bisher könnten derartige Merkmale auch dann gespeichert werden, wenn sie z. B. von nur einer befragten Referenzperson angegeben worden seien, andere Quellen die Information aber nicht bestätigen konnten. Dadurch habe es zur Speicherung von Merkmalen,

die im Abschlußbericht des Bundesamtes für Verfassungsschutz an den Geheimschutzbeauftragten mangels Relevanz nicht enthalten gewesen seien, kommen können.

— Im Abschlußberichts-Entwurf sei jeweils am Rand die Fundstelle in der Akte zu vermerken, an der sich der Beleg für die jeweilige Information befinde. Bislang sei es z. T. schwierig gewesen, aus den Akten nachzuvollziehen, warum ein bestimmtes Merkmal vergeben worden sei.

— In Zukunft würden die Merkmale durch Vergabe eines sog. „EK-Datums" zeitlich zugeordnet. Bislang sei aus dem Datensatz nicht zu erkennen gewesen, wie lange das jeweilige Ereignis zurückgelegen habe, das Grundlage für die Speicherung des Merkmals gewesen sei.

— In Zukunft würden die Sachbearbeiter der Abteilung V bei der Einzelabfrage vom Terminal aus nur noch die Personengrunddaten, die Tatsache der Überprüfung sowie das Ergebnis der Überprüfung (abgelehnt/nicht abgelehnt) erhalten — ausgenommen für Zwecke der Dateneingabekontrolle. Bisher seien bei jeder Abfrage sämtliche belastenden Merkmale mit ausgegeben worden.

— Auf die sonstigen noch verbliebenen Merkmale könne nur noch im Rahmen von Querschnittauswertungen/Suchmaßnahmen zugegriffen werden. Diese Auswertungen seien nur für Zwecke des vorbeugenden personellen Geheimschutzes sowie der Spionageabwehr zulässig. Sie müßten vom Abteilungsleiter V genehmigt werden. Sie seien in nachprüfbarer Weise zu protokollieren.

— Aus der Datei PUD würden außer an die Abteilung IV keine Daten übermittelt. Es werde allenfalls im Einzelfall Auskunft aus der Akte erteilt. Bislang sei nicht sichergestellt gewesen, daß PUD-Datensätze nicht auch in andere Fachabteilungen gelangen konnten.

— Das Bundesamt für Verfassungsschutz prüfe, ob die vom Bundesbeauftragten für den Datenschutz zur Erhöhung der Datensicherheit gemachten Vorschläge umgesetzt werden könnten. In jedem Falle werde jeder einzelne Datensatz als Verschlußsache VS-Nur für den Dienstgebrauch sowie die Gesamtheit der Datensätze als Verschlußsache VS-VERTRAULICH eingestuft.

— Zwischen Bundesamt für Verfassungsschutz und Bundesbeauftragtem für den Datenschutz würden Gespräche darüber stattfinden, welche Maßnahmen zu ergreifen seien, solange noch Datensätze in der alten PUD-Datei gespeichert seien. Nach einer Schätzung des Bundesamtes für Verfassungsschutz dürfte es etwa fünf Jahre dauern, bis der Datenbestand in PUD-alt abgebaut werden könne.

— Zum neuen Codierplan werde es eine Arbeitsanweisung geben, in der näher definiert sei, unter welchen Voraussetzungen die jeweiligen Merkmale gespeichert werden dürften. An der Erarbeitung dieser Arbeitsanweisung werde der Bundesbeauftragte für den Datenschutz beteiligt. Bislang sei zwischen dem Bundesbeauftragten für den Datenschutz, dem Bundesminister des Innern und dem Bundesamt für Verfassungsschutz folgendes abgesprochen:

— Bei Hinweisen auf (frühere oder heutige) Mitgliedschaft/Betätigung in einer verfassungsfeindlichen Organisation führe das Bundesamt für Verfassungsschutz in der Regel eine Befragung der betroffenen Person durch. Nur wenn sich herausstelle, daß eine solche Verbindung tatsächlich bestanden habe oder bestehe und daß diese (zum Zeitpunkt der Sicherheitsüberprüfung) sicherheitserheblich sei, erfolge eine Speicherung.

— Strafbare Handlungen würden nur gespeichert, soweit sich daraus eine Gefährdungssituation ableiten lasse (z. B. Erpreßbarkeit, falls frühere Straftat dem heutigen Lebensumfeld nicht bekannt sei) oder aus der Tat Zweifel an der Zuverlässigkeit nach § 4 Abs. 2 Nr. 1 SiR erwüchsen.

— Umstände im Umfeld der betroffenen Person müßten auf diese sicherheitsmäßig „durchschlagen", um sicherheitserheblich zu sein. In der Regel komme dies nur bei Personen in Betracht, zu denen in der Sicherheitserklärung Angaben verlangt würden.

— Der Bundesminister des Innern, das Bundesamt für Verfassungsschutz und der Bundesbeauftragte für den Datenschutz seien übereinstimmend der Auffassung, daß mit diesen Maßnahmen alle wichtigen Beanstandungen und Kritikpunkte im Prüfbericht des Bundesbeauftragten für den Datenschutz in bezug auf die PUD ausgeräumt seien. Die vorgesehenen Maßnahmen verbesserten darüber hinaus die Qualität der Datenverarbeitung bei der Abteilung V des Bundesamtes für Verfassungsschutz und stellten deshalb auch einen Sicherheitsgewinn dar.

Die Koalitionsfraktionen und die Fraktion der SPD zeigten sich erfreut über die zwischen dem Bundesbeauftragten für den Datenschutz und der Bundesregierung erzielten Einigungen.

Die Fraktion DIE GRÜNEN griff demgegenüber die Aussage auf, daß aus der Datei PUD außer an die Abteilung IV keine Daten übermittelt würden und allenfalls im Einzelfall Auskunft aus der Akte erteilt werde. Die Ausnahmen von der Zweckbindung „im Einzelfall" müßten sofort gestrichen werden. Das Bundesministerium des Innern werde aufgefordert, die neugefaßte Richtlinie/Dienstvorschrift bez. dieses Bereiches dem Innenausschuß vorzulegen. Ebenso sei über die Maßnahmen zur Löschung des PUD-Altbestandes dem Innenausschuß zu berichten. Um überprüfen zu können, ob nicht auch heute noch die nach überholtem Recht strafbaren homosexuellen Beziehungen gemäß §§ 175ff. StGB gespeichert würden, müsse dem Innenausschuß der Kodierplan sofort nach seiner Erstellung überreicht werden.

5.4 *Übernahme der Grundsätze von PUD für den Militärischen Abschirmdienst*

Der Bundesbeauftragte für den Datenschutz legte bei den Beratungen dar, die gemeinsame Lösung, die man für PUD im Bereich des Bundesamtes für Verfassungsschutz gefunden habe, sei geeignet, vom Militärischen Abschirmdienst übernommen zu werden. Sein Vorschlag fand die Zustimmung der Koalitionsfraktionen und der Fraktion der SPD.

Die Bundesregierung berichtete in der Sitzung des Innenausschusses am 7. Dezember 1988, die Bestimmungen über die Speicherung von Daten in der Personenzentraldatei des Militärischen Abschirmdienstes, Segment Merkmalspeicherung, seien in enger Abstimmung mit dem Bundesbeauftragten für den Datenschutz überarbeitet worden. Die Grundsätze der PUD-Datei seien soweit wie möglich übernommen worden: Man müsse jedoch bedenken, daß die Organisation des Bundesamtes für Verfassungsschutz sich von der des Militärischen Abschirmdienstes grundsätzlich unterscheide. Beim Bundesamt für Verfassungsschutz seien in einem Haus die Elemente der Informationsbeschaffung und Registrierung untergebracht. Beim Militärischen Abschirmdienst habe man eine Zentrale in Köln; die Informationsbeschaffung werde von 35 Dienststellen wahrgenommen, die einen Zugang zu den Daten unter gewissen Auflagen haben müßten. Unter Berücksichtigung dieses besonderen Umstandes habe man die Bestimmungen überarbeitet. Es seien Merkmalbereiche reduziert bzw. völlig gestrichen worden. Die inhaltliche und nutzungstechnische Konzeption von PUD sei in Übereinstimmung mit dem Bundesbeauftragten für den Datenschutz auf die Personenzentraldatei des Militärischen Abschirmdienstes übertragen worden.

Der Bundesbeauftragte für den Datenschutz bestätigte, daß hinsichtlich der Übersetzung der PUD auf den Militärischen Abschirmdienst Einvernehmen mit der Bundesregierung bestehe.

5.5 *Bundeskriminalamt: Verfahren bei der Anlegung von Kriminalakten und der Festsetzung des Aussonderungsprüfdatums*
(siehe Kapitel 13.1 des Neunten Tätigkeitsberichts)

Die Bundesregierung erwiderte auf die Kritik des Bundesbeauftragten für den Datenschutz, die Einrichtung einer zentralen Serviceeinheit habe sich in der Praxis bewährt, zumal die Beamten entsprechend geschult seien und die Fachbereiche die Möglichkeit der Überprüfung hätten. Das Bundeskriminalamt habe durch eine amtsinterne Weisung veranlaßt, daß die Aussonderungsprüffristen in Zukunft manuell und unabhängig vom Tag des Ereignisses vergeben würden.

Die Koalitionsfraktionen, die Fraktion der SPD und die Fraktion DIE GRÜNEN forderten den Bundesbeauftragten für den Datenschutz auf, anhand von Stichproben zu überprüfen, ob durch dieses Verfahren seinen Bedenken Rechnung getragen sei.

5.6 *Bundeskriminalamt: Speicherungen von „anderen Personen" in der Arbeitsdatei PIOS-Rauschgift (APR)*
(siehe Kapitel 13.1 des Neunten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz)

Der Datenschutzbeauftragte erklärte hierzu vor dem Innenausschuß, er hege anhand der Statistik der Arbeitsdatei PIOS-Rauschgift (APR), nach der in dieser Datei insgesamt ca. 67 000 Beschuldigte und Verdächtige, aber nur ca. 500 „andere Personen" gespeichert gewesen seien, die Vermutung, daß in der Arbeitsdatei PIOS-Rauschgift unter Umgehung der strengeren Datenschutzvorschriften für „andere Personen" viele Personen als „Verdächtige" eingestuft würden. Man habe die Richtigkeit dieser Vermutungen jedoch noch nicht durch Prüfungen verifizieren können.

Die Bundesregierung betonte demgegenüber, daß die Vermutung des Bundesbeauftragten für den Datenschutz nicht bestätigt werden könne. Man habe für eine Reihe von Daten die Prozentsätze für die Speicherung Beschuldigter, Verdächtiger und anderer Personen auswerfen lassen. Der Prozentsatz der Beschuldigten und Verdächtigen sei von Datei zu Datei verschieden. In der APIS-Datei sei der Prozentsatz der Verdächtigen relativ niedrig, in der Datei PIOS-Rauschgift z. B. sehr hoch. Dies zeige nur, daß das Stadium der Ermittlungen im Speicherungszeitpunkt unterschiedlich sei.

Die Koalitionsfraktionen führten aus, es bleibe abzuwarten, ob Stichprobenüberprüfungen die Vermutung des Bundesbeauftragten für den Datenschutz bestätigten oder widerlegten. Sie vermuteten jedoch, daß die Problematik z. B. auch bei der Datei „Landfriedensbruch und verwandte Straftaten" auftreten werde, falls die Erfassungskriterien dieser Datei ausgeweitet würden.

Die Bundesregierung erwiderte darauf, die Konferenz der Innenminister und -senatoren der Länder habe eine Ausweitung der Erfassungskriterien für die Datei „Landfriedensbruch und verwandte Straftaten" abgelehnt, die von einer Ad-hoc-Arbeitsgruppe des Arbeitskreises II vorgeschlagen worden sei. Es sei jedoch eine Verlängerung der Speicherungsfristen von drei auf fünf Jahre beschlossen worden und eine vereinfachte Zurverfügungstellung dieses gesonderten Bestandes in der Fahndungsdatei von INPOL. Sie gab in der Sitzung des Innenausschusses am 18. Januar 1989 einen Bericht über die Erfassungskriterien und die Praxis bezogen auf die Datei „Landfriedensbruch und verwandte Straftaten" ab, der diese Angaben erneut bestätigte, und legte dar, meldepflichtig sei insoweit die Einleitung von Ermittlungsverfahren z. B. wegen Landfriedensbruchs, schweren Hausfriedensbruchs, Straftaten mit Gewalttätigkeiten und gemeingefährlichen Straftaten, soweit die Tatbegehung in einen örtlichen, zeitlichen oder sachlichen Zusammenhang mit einem Demonstrationsgeschehen stehe.

Die Fraktion der SPD regte an, das seitens des Bundesbeauftragten für den Datenschutz unter Ziffer 13.1 seines Neunten Tätigkeitsberichts angesprochene

Thema solle nach Durchführung einer Prüfung durch den Bundesbeauftragten wieder im Innenausschuß aufgegriffen werden.

Die Fraktion DIE GRÜNEN stimmte dem Vorschlag der Fraktion der SPD zu. Sie verwies auf die Forderungen, die der Bundesbeauftragte für den Datenschutz bereits im Kapitel 12.4 seines Achten Tätigkeitsberichts aufgestellt habe, und betonte, es sei unklar, ob diesen Forderungen, wonach dringend zwischen „Beschuldigten", „Verdächtigen" und „anderen Personen" zu differenzieren sei, nachgekommen worden sei.

5.7 *Bundesnachrichtendienst*

Zu Kapitel 15 des Neunten Tätigkeitsberichts wurde seitens des Bundesbeauftragten für den Datenschutz und der Bundesregierung erklärt, daß der Bundesnachrichtendienst mittlerweile den Entwurf einer Dienstvorschrift erstellt habe, in der festgelegt sei, wie der von der Datenverarbeitung betroffene Personenkreis umschrieben und eingegrenzt werden solle. Die Beratung dieses Entwurfs sei vorgesehen.

Schwierigkeiten ergäben sich hinsichtlich der Bildung von Kategorien. Es sei problematisch, einen Restbestand zu vermeiden, der unter die Kategorie „Sonstiges" gefaßt werden müsse.

Seitens des Bundesbeauftragten für den Datenschutz wurde betont, es sei wichtig — unabhängig von einer gesetzlichen Regelung — auch im Bereich des Bundesnachrichtendienstes etwas einer Errichtungsanordnung Ähnliches an der Hand zu haben, damit insbesondere seitens des Bundesbeauftragten für den Datenschutz bekannt sei, mit welchem Personenkreis man es zu tun habe.

Die Koalitionsfraktionen und die Fraktion der SPD stimmten dem Bundesbeauftragten für den Datenschutz zu.

Die Fraktion DIE GRÜNEN regte eine ausführlichere Beratung des Bereiches Bundesnachrichtendienst in Zusammenhang mit den nächsten Tätigkeitsberichten des Bundesbeauftragten für den Datenschutz an.

5.8 *Bundesgrenzschutz*

Der Bundesbeauftragte für den Datenschutz behandelt den Bereich Bundesgrenzschutz in Kapitel 11.1.2 seines Achten und Kapitel 16 seines Neunten Tätigkeitsberichts.

Die Koalitionsfraktionen, die Fraktion der SPD und die Fraktion DIE GRÜNEN trafen folgende Übereinkunft:

Da über den Bereich Bundesgrenzschutz seitens des Bundesbeauftragten für den Datenschutz im Zusammenhang mit dem Zehnten Tätigkeitsbericht ein Prüfbericht erstellt worden sei, solle insoweit im Zusammenhang mit dem Zehnten Tätigkeitsbericht intensiv in die Beratungen eingestiegen werden.

Seitens des Bundesbeauftragten für den Datenschutz wurde darauf hingewiesen, daß der im Neunten Tätigkeitsbericht aufgeführte Vorgang — Anlegung einer Namensliste über jugendliche Mitglieder des Deutschen Alpenvereins, die auf DDR-Gebiet demonstriert hatten — bereinigt worden sei. Die Liste sei aus den Akten entfernt worden.

5.9 *Kreditsicherung*

Zum Thema Kreditsicherung, das der Bundesbeauftragte für den Datenschutz in Kapitel 15.1 seines Achten und Kapitel 19.1 seines Neunten Tätigkeitsberichts anspricht, verwies die Fraktion der SPD auf den Entwurf eines Gesetzes zum Schutz personenbezogener Informationen (Bundes-Informationsschutzgesetz — BISG) — Drucksache 11/3730. Sie erklärte, im Bereich der SCHUFA müsse insbesondere die Frage der Einbeziehung der Betroffenen, Probleme in Verbindung mit Änderungen des Datensatzes sowie die Frage der Kostenabwälzung auf die Betroffenen im Zusammenhang mit bevorstehenden Beratungen zur Novellierung des Bundesdatenschutzgesetzes erörtert werden.

Die Fraktion DIE GRÜNEN schlug vor, die SCHUFA völlig abzuschaffen, da die Nachteile, die den betroffenen Kunden hierdurch entstünden, zu groß seien.

Die Koalitionsfraktionen sahen hinsichtlich des Themas Kreditsicherung keinen Beratungsbedarf.

5.10 *Verkehrszentralregister: Auskunfterteilung nach § 30 StVG*

Zu dem seitens des Bundesbeauftragten für den Datenschutz in Kapitel 9.2.2 angesprochenen Bereich wünschte die Fraktion der SPD nähere Auskünfte durch die Bundesregierung.

Die Bundesregierung legte dar, der Bundesminister für Verkehr, die Bundesländer und der Bundesbeauftragte für den Datenschutz hätten sich über eine Regelung verständigt, die noch vor der geplanten Novellierung der Vorschriften über das Verkehrszentralregister verwirklicht werden solle. Danach werde eine Teilauskunft zum einen in dem praktisch wichtigen Fall der Ausstellung eines Ersatzführerscheins erteilt und zum anderen in dem Fall der Ausgabe von roten Kennzeichen zur wiederkehrenden Verwendung. Zudem werde in folgenden Fällen auf eine Anfrage beim Verkehrszentralregister gänzlich verzichtet: bei der Anerkennung als Sehteststelle nach der StVZO und bei der Anerkennung von Stellen zur Ausbildung in Erster Hilfe und für Sofortmaßnahmen am Unfallort. Diese Vorabregelung werde am 1. Juni 1989 in Kraft treten. Eine frühere Anwendung sei nicht möglich, weil hierzu noch verschiedene Programmänderungen durchzuführen seien.

Die Fraktion DIE GRÜNEN sah insoweit großen Beratungsbedarf gegeben.

5.11 Kfz-Zulassungsdateien: Übermittlung an die Automobilindustrie

Die Fraktion der SPD wünschte nähere Auskünfte über den vom Bundesbeauftragten für den Datenschutz in Kapitel 9.3.2 des Neunten Tätigkeitsberichts angesprochenen Problemkreis. Die Bundesregierung betonte, die Beanstandungen des Bundesbeauftragten für den Datenschutz seien noch in den Zeitraum vor Inkrafttreten des Änderungsgesetzes zum Straßenverkehrsgesetz gefallen. In diesem Gesetz sei klargestellt worden, daß eine Datenübermittlung an die Automobilindustrie nur für Zwecke von Rückrufmaßnahmen zulässig sei. Der Verkehrsminister habe das Kraftfahrtbundesamt damals angewiesen, die bisherige Datenlieferung einzustellen. Dies sei geschehen. Derzeit fänden erneute Gespräche auf einer anderen Grundlage statt, bezogen darauf, daß der Käufer eines Neufahrzeuges in die Datenübermittlung einwillige. Der Bundesbeauftragte für den Datenschutz wies darauf hin, daß letzteres Thema in seinem Elften Tätigkeitsberichts angesprochen werde.

6. Nach Ansicht der Fraktion DIE GRÜNEN bestehender zusätzlicher Beratungsbedarf

Die Fraktion DIE GRÜNEN regte zunächst an, folgende von ihr aufgelisteten Punkte, die anläßlich des Achten und Neunten Tätigkeitsberichts noch nicht erörtert worden seien, ebenfalls vorab im Berichterstatterkreis (Liste 1) bzw. im Innenausschuß (Liste 2) zu beraten. Als die Mehrheit der anderen Fraktionen dem nicht zustimmte, schlug sie vor, diese Themen jedenfalls im Zusammenhang mit dem Zehnten und Elften Tätigkeitsbericht zu behandeln.

Liste 1
„Nicht angesprochene Probleme
aus dem Achten Tätigkeitsbericht des BfD

1. BKA

a) Ähnlich wie in der Staatsschutz-Abteilung (Seite 46 R): stärkere Berücksichtigung von bzw. aktive Erkundigungspflicht des BKA nach speicherungsrelevanten Vorgängen wie Gerichtsentscheidungen etc. auch in der Drogenabteilung (Seite 35 L)

b) Einhaltung der Benachrichtigungspflicht und der Pflicht zur Löschung von Daten Unbeteiligter nach Abschluß einer Telefonabhörmaßnahme gemäß §§ 100a, 100b StPO (35 R) und Erfahrungen mit der eingeführten besonderen Kennzeichnung der durch TÜ bekanntgewordenen Personalien (9/58 R)

c) Einhaltung der Pflicht zur Löschung gespeicherter Daten von Vermißten nach Abschluß der Fahndung nach ihnen (35 R)

d) Verbesserte Vorkehrungen zur Verhinderung des ausländischen Gebrauchs von im Interpol-Verkehr übermittelten Daten entsprechend dem Verbot des § 51 BZRG (35 R). Inhalt der neuen Interpol-Übermittlungs-„Richtlinien von 1984" in diesem Zusammenhang?

e) Nachberichtspflicht des BKA an ausländische Datenempfänger (35 R) entsprechend den BMI-Vorschlägen im Rahmen des Schengener Abkommens (vgl. Stellungnahme der Bundesregierung — nachfolgend „BR" — zum 8. TB, Seite 47). Heutige Praxis?

f) „Kritische Bestandsaufnahme" (37 R) der EDV-Struktur, insbesondere INPOL

  aa) Differenzierung und Begrenzung der Zugangsberechtigung zu einzelnen Dateien zur Verhinderung von grundsätzlich dateiübergreifenden Recherchen (42 L), auch außerhalb der FDR (vgl. BE-Zwischenbericht S. 13)

  bb) Beachtung (kürzerer) Löschungsfristen auch bei andauernder Speicherung einer Person in einer anderen Datei mit längerer Löschungsfrist (42 L)

  cc) Aushöhlung des KAN-Konzepts (vgl. hierzu 9/82 Nr. 21; BR 8/52)

  - Zugang von nach KAN nicht anfrageberechtigten Polizeidienststellen zu beim BKA zentral gespeicherten ED-Unterlagen (43 R)
  - Zugriff nicht nur der Drogenabteilungen, sondern aller KAN-Berechtigten auf Daten über regionale Drogen-Kleinkriminalität in der FDR (43 R)
  - Zu viele, zu schnell angelegte und lückenhafte Kriminalakten im Rahmen des BKA-AN (44)

g) Speicherung „anderer Personen" auch außerhalb von APR

- Erwägungen und Beschlüsse der Beratungen von AG Kripo und AK II der IMK (46 L)
- Durchgängige Benachrichtigung „Anderer Personen" über Speicherung auch im TE-Bereich (46 L; vgl. auch 9/82 Nr. 23)
- Differenzierung zwischen „Beschuldigten" und „Verdächtigen" bez. der Speicherfrist (46 R)

2. BfV

a) Grundsätzlicher Verzicht auf die Übermittlung löschungsreifer Daten (48 L)

b) Grundsätzlicher Verzicht auf personenbezogene Daten in Hintergrundakten über „beeinflußte Organisationen" (48 L)

c) Verkürzung der Regelspeicherzeit von 15 Jahren zumindest in den Extremismus-Abteilungen (48 L). Wie viele Erstspeicherungen als begrenzte Zeitspeicherungen von 2 bis 5 Jahren (vgl. BR 8/56)?

d) Verzicht auf besondere Identifizierungsdateien (welche?) in den Extremismus-Abteilungen (48 R, 49)

e) Inhalt des 1987/88 zu realisierenden Konzepts dieser Personenarbeitsdateien PAD (48 R)? (Unterrichtung zugesagt in BR 8/57)

3. Sicherheitsbehörden allgemein: Internationale Datenübermittlung

a) Ausnahmsweise Durchbrechung der Zweckbindung durch ausländischen Datenempfänger nur mit Zustimmung der deutschen übermittelnden Stelle

b) Übermittlung nur bei einheitlichen Überprüfungs- bzw. Löschungsfristen und einem Mindestmaß an Auskunftsrechten

c) Vermeidung der Übermittlung ausländischer Daten an deutsche Stellen ohne eigene Erhebungsbefugnisse (alle 40 L)

Nicht angesprochene Probleme
aus dem Neunten Tätigkeitsbericht

1. BKA

a) Ergebnis der vom BMI zugesagten (BR 9/40) Überprüfung des BKA-AN?

b) Im BKA ergriffene Maßnahmen aufgrund der Zusage (BR 9/42), Mängel insbesondere bei kurzfristig erstellten SPUDOK-Errichtungsanordnungen zu vermeiden?

2. BfV

Ergänzend zu den ab 1. Mai 1988 geltenden Sicherheitsüberprüfungsrichtlinien Vorkehrungen für eine strikte Zweckbindung und Präzisierung der Datenübermittlung zwischen BfV und Geheimschutzbeauftragten (57)

3. BND

Zukünftige Gewährung ungehinderter Kontrollen durch den BfD (63)"

Liste 2

„1) Ausländerzentralregister

2) ZEVIS

3) Bundeszentralregister

4) Mikrozensus

5) Telekommunikation

6) Bundesamt für Verfassungsschutz

a) Vielfalt der außer der Personenzentraldatei geführten automatischen Dateien

b) Gebotene Straffung und Differenzierung der Löschungsfristen aufgrund der NADIS-Löschungsrichtlinien

c) Personenüberprüfungsdatei PUD des BfV Abt. V: Probleme der neuen Errichtungsanordnung, des Kodierplans und der Arbeitsanweisung hierzu

d) Datenübermittlungen ins Ausland: Befugnisse der LfV — Frage des „Berliner Lochs im Datenschutz"

7) Bundeskriminalamt

a) Aushöhlung des KAN-Konzepts

b) Probleme einzelner Dateien

— Terroristisches Schrifttum TESCH

— Arbeitsdatei PIOS Gefährdung APG

— PKK

— Walter

— Schacht

— Arbeitsdatei Kriminelle Vereinigungen

— Arbeitsdatei PIOS Organisierte Kriminalität APOK

— Arbeitsdatei PIOS Landfriedensbruch

— Arbeitsdatei PIOS Meldedienst Staatsschutz APMS

— SPUDOK Bewegung

— SPUDOK Startbahn 18 West

— Personenrecherchiersystem PERES

— BKA-Aktennachweis AN"

Die Fraktion DIE GRÜNEN regte zudem an, das Thema Erfassung von Fluggästen i. S. einer Erstellung von Bewegungsbildern zu beraten.

Bonn, den 11. September 1989

Dr. Blens **Dr. Hirsch** **Wartenberg (Berlin)** **Frau Dr. Vollmer**

Berichterstatter

DER BUNDESMINISTER DES INNERN

Bonn, den 27. August 1986

Stellungnahme der Bundesregierung zu dem Achten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (BfD)

Der Deutsche Bundestag hat die Bundesregierung ersucht, dem Innenausschuß zu Beanstandungen, Forderungen, Anregungen und Rechtsauffassungen des Bundesbeauftragten für den Datenschutz, soweit ihnen nach Berichtsvorlage noch nicht Rechnung getragen worden ist oder an anderen Rechtsauffassungen festgehalten werden soll, eine Stellungnahme zuzuleiten und darin die Haltung der Bundesregierung im einzelnen darzulegen und zu begründen (vgl. Nummer 1.4 des Beschlusses des Deutschen Bundestages vom 9. Juni 1982, Drucksache 9/1623).

Die hiermit vorgelegte Stellungnahme der Bundesregierung ist in ihrem Aufbau entsprechend der Systematik des Achten Tätigkeitsberichts gegliedert.

Zu 2. Innere Verwaltung

Zu 2.1. Neue Personalausweise und Pässe

Der Bundesbeauftragte für den Datenschutz befaßt sich erneut mit der bereits in früheren Tätigkeitsberichten dargelegten Problematik der Einführung des fälschungssicheren und maschinenlesbaren Personalausweises.

Die Bundesregierung bemerkt hierzu, daß nach der inzwischen erfolgten Verkündung der Novelle zum Personalausweisgesetz und dem neuen Paßgesetz vom 19. April 1986 (BGBl. I S. 537 ff.) ab 1. April 1987 fälschungssichere und maschinenlesbare Personalausweise sowie ab 1. Januar 1988 fälschungssichere und maschinenlesbare Reisepässe in der Bundesrepublik Deutschland ausgegeben werden. Die Gesetze enthalten die nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 erforderlichen datenschutzrechtlichen Bestimmungen. An den Beratungen der Gesetzentwürfe im Innenausschuß und im Rechtsausschuß des Deutschen Bundestages war der Bundesbeauftragte für den Datenschutz beteiligt.

Zu 2.3. Ausländerzentralregister

Das Verfahren der vom Bundesminister des Innern zur Vorbereitung einer neuen Konzeption des Ausländerzentralregisters eingesetzten Arbeitsgruppe wird vom Bundesbeauftragten für den Datenschutz positiv beurteilt.

Der inzwischen erarbeitete Abschlußbericht, der die Beratungsergebnisse der Arbeitsgruppe enthält, beinhaltet außer Vorschlägen über die künftig zu führenden Datenfelder sowie die Datenanlieferung und -übermittlung auch eine Auflistung des Bedarfs an rechtlichen Regelungen. Der Bericht ist nunmehr mit den Bundesressorts und den Bundesländern abzustimmen. Dabei wird der Bundesbeauftragte für den Datenschutz fortlaufend beteiligt.

Zu 2.4. Wahlrecht

Der Bundesbeauftragte für den Datenschutz hält das Verfahren, daß sich Gemeinden bzw. örtliche Wahlleiter an Behörden mit der Bitte um Benennung von Beschäftigten zur Bestellung von Wahlvorständen wenden, nur dann für sinnvoll, wenn sich nicht auf freiwilliger Basis geeignete Personen für diese Ehrenämter finden lassen. Er empfiehlt, die Problematik durch Rechtsnormen im Bundeswahlgesetz oder in der Bundeswahlordnung noch rechtzeitig vor der nächsten Bundestagswahl zu regeln.

Der Bundesminister des Innern führt hierzu aus, daß nach § 11 des Bundeswahlgesetzes die Beisitzer der Wahlausschüsse und die Mitglieder der Wahlvorstände ihre Tätigkeit ehrenamtlich ausüben. Zur Übernahme dieses Ehrenamtes ist grundsätzlich jeder Wahlberechtigte verpflichtet; das Ehrenamt darf nur aus wichtigem Grund abgelehnt werden.

Aus dieser Vorschrift läßt sich kaum die Pflicht einer Behörde ableiten, einer Wahlbehörde Listen ihrer Bediensteten mit detaillierten Personalangaben zur Verfügung zu stellen. Aus wahlorganisatorischer Sicht halten die Bundesregierung und die überwiegende Mehrheit der Länder sowie der Bundeswahlleiter eine Benennungspflicht der Behörden bis auf weiteres nicht für notwendig. Vielmehr wird es für die Gewinnung von Personen zur Übernahme eines Wahlehrenamtes als ausreichend angesehen, wenn Dienststellen ihre Beschäftigten auf den Aufruf von Wahlbehörden zur Übernahme eines Wahlehrenamtes hinweisen mit der Empfehlung, sich — soweit möglich — hierfür freiwillig zur Verfügung zu stellen.

Demzufolge besteht derzeit für eine spezifisch wahlrechtliche Regelung kein Bedürfnis.

Zu 3. Rechtswesen

Zu 3.1. Bundeszentralregister

Der Bundesbeauftragte für den Datenschutz hat beim Bundeszentralregister (BZR) auch im Jahre 1985 einen Kontrollbesuch durchgeführt und „hierbei ein insgesamt erfreulich hohes Niveau des Datenschutzes in dieser Behörde festgestellt".

Die in früheren Tätigkeitsberichten des BfD enthaltenen Empfehlungen zur Novellierung des Bundeszentralregistergesetzes (BZRG) sind vom Bundesminister

der Justiz mit dem Bundesbeauftragten für den Datenschutz erörtert worden. Dabei hat der Bundesbeauftragte für den Datenschutz seine Empfehlungen erläutert und aktualisiert (vgl. auch Nummer 19.4 — Bilanz — Achter Tätigkeitsbericht). Nach Mitteilung des Bundesministers der Justiz werden die aktualisierten Empfehlungen des Bundesbeauftragten für den Datenschutz noch eingehend geprüft. Sobald die Stellungnahmen der zu beteiligenden Landesregierungen und der übrigen betroffenen Stellen vorliegen, wird beurteilt werden können, in welcher Weise die Empfehlungen des Bundesbeauftragten für den Datenschutz bei einer weiteren Novellierung des BZRG berücksichtigt werden können.

Zu 3.2. Mitteilungen in Zivilsachen

Der Bundesbeauftragte für den Datenschutz begrüßt, daß die Mitteilungen in Zivilsachen (MiZi) im Gerichtsverfassungsgesetz gesetzlich geregelt werden sollen.

Nach Erarbeitung des entsprechenden Gesetzentwurfs wird der Bundesbeauftragte für den Datenschutz die erbetene Gelegenheit zur Stellungnahme erhalten.

Zu 3.3. Schuldnerverzeichnis

Der Bundesbeauftragte für den Datenschutz weist erneut auf die Notwendigkeit hin, den Datenschutz bei der Übermittlung von Angaben aus dem Schuldnerverzeichnis zu verbessern, insbesondere den Umfang der praktizierten Datenübermittlungen kritisch zu überprüfen und auch die zugrundeliegende gesetzliche Regelung des § 915 ZPO zu überarbeiten.

Der Bundesminister der Justiz bemerkt hierzu, daß er bemüht ist, die Auskünfte aus dem Schuldnerverzeichnis den Erfordernissen des Datenschutzes anzupassen.

Nach ausführlichen Erörterungen mit den Landesjustizverwaltungen, dem Bundesbeauftragten für den Datenschutz und den Spitzenverbänden der Wirtschaft hat der Bundesminister der Justiz im August 1985 einen Entwurf zur Änderung gesetzlicher Vorschriften über das Schuldnerverzeichnis sowie den Entwurf einer Verordnung über die Erteilung von Abdrucken aus dem Schuldnerverzeichnis vorgelegt. Nach den vorangegangenen Erörterungen konnte davon ausgegangen werden, daß die Entwürfe sowohl den Anforderungen des Datenschutzes als auch den Bedürfnissen der Wirtschaft gerecht werden würden, so daß sie noch im Laufe dieser Legislaturperiode — etwa im Rahmen eines bereits eingebrachten Gesetzentwurfs — hätten parlamentarisch beraten und verabschiedet werden können. Auch in später eingehenden Stellungnahmen zu den Entwürfen wurde die Notwendigkeit eines sachgerechten und praxisnahen Ausgleichs zwischen Datenschutz und Gläubigerschutz weitgehend anerkannt, wenn auch einige Wirtschaftsorganisationen einen Regelungsbedarf verneinten. Die Entwürfe wurden jedoch von den für Datenschutz zuständigen Stellen in entscheidenden Punkten abgelehnt. Daraufhin wurde auch in der Wirtschaft wieder Kritik an den Entwürfen laut.

Der Bundesminister der Justiz bemüht sich nachdrücklich, die Entwürfe zu einem akzeptablen Kompromißvorschlag fortzuentwickeln. Bei den noch bestehenden Differenzen wird es allerdings schwerlich möglich sein, noch in dieser Legislaturperiode eine Neuregelung über das Schuldnerverzeichnis zu verwirklichen.

Zu 5. Personalwesen

In der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkt 7.3) wird die Bundesregierung aufgefordert, über den Stand ihrer Überlegungen zur Regelung des Personalaktenrechts des Bundes zu berichten:

Der Bundesminister des Innern nimmt hierzu wie folgt Stellung:

I.

Rechtsgrundlage für das Personalaktenwesen der Beamten des Bundes ist § 90 BBG, für den Tarifbereich des öffentlichen Dienstes § 13 BAT, § 13a MTB II. Die Vorschriften setzen die Befugnis und Pflicht zur Führung von Personalakten voraus; sie regeln das Recht der Beschäftigten zur Einsicht in seine Personalakten und konkretisieren den Grundsatz des rechtlichen Gehörs. Darüber hinaus hat die Rechtsprechung Grundsätze zum Personalaktenrecht entwickelt, die sich nicht unmittelbar aus der gesetzlichen Vorschrift ergeben. Das Volkszählungsurteil des Bundesverfassungsgerichts hat zusätzlich Fragestellungen aufgeworfen und Erwartungen geweckt. Ergänzt werden die Rechtsvorschriften durch umfangreiche, unter den verschiedensten Bezeichnungen laufenden Erlasse zur Führung und Verwaltung von Personalakten. Die Entwicklung hat insgesamt zu einer unübersichtlichen Kasuistik geführt, die weder der Rechtsklarheit noch der Rechtssicherheit dient und nicht alle Regelungslücken befriedigend zu schließen vermag. Aus diesem Grunde beabsichtigt die Bundesregierung, das Personalaktenwesen auf eine neue gesetzliche Grundlage zu stellen und die organisatorischen Richtlinien zur Führung und Verwaltung der Personalakten zu modernisieren. Sie weiß sich darin mit dem Bundesbeauftragten für den Datenschutz einig.

Oberstes Ziel der Neuordnung, die im engsten Einvernehmen mit den Ländern erfolgen soll, wird die Sicherung der Persönlichkeitsrechte der Beschäftigten bei der Führung der Personalakten sein. Die Beachtung dieses Grundsatzes ist zwar für die Personalverwaltungen nichts grundlegend Neues, weil bisher schon z. B. die Pflicht zur Verschwiegenheit, die Beschränkung der Weitergabe von Personalakten sowie andere Schutzmaßnahmen zu den selbstverständlichen Prinzipien einer rechtsstaatlichen Personalaktenführung gehören. Es dient jedoch der Rechtssicherheit, wenn in einer modernisierten Systematik die Bestätigung bestehender Pflichten, die Umsetzung der von der Rechtsprechung entwickelten Grundsätze zum

Schutz der Persönlichkeitsrechte sowie notwendige Ergänzungen, die durch Nutzung neuer Informationstechnologien für die Personalverwaltung erforderlich werden, erfolgen. Die Bundesregierung ist sich dabei bewußt, daß ein rechtsstaatlich vertretbarer Ausgleich zwischen der Wahrung der Persönlichkeitsrechte und der Erhaltung der Funktionsfähigkeit des Personalaktenwesens als wesentliches Hilfsmittel einer effizienten Personalwirtschaft und -verwaltung herzustellen ist. Bisherige Gestaltungen automatisierter Personalverwaltungssysteme beweisen, daß es sehr gut möglich ist, beim Einsatz moderner Informationstechnologien einen Ausgleich zwischen den Chancen neuerer technischer Entwicklungen und den Vorkehrungen gegen mögliche Gefahren zu erzielen.

Im Zusammenhang mit der gesetzlichen Neuregelung des Personalaktenrechts verfolgt die Bundesregierung das weitere Ziel, die Effizienz der Personalaktenverwaltung zu erhöhen. Auf Anregung und in Zusammenarbeit mit dem Bundesrechnungshof wird die Bundesregierung die Vorschriften über das Führen und Verwalten von Personalakten vereinheitlichen und modernisieren.

II.

Ein stark ansteigendes Problembewußtsein bei Personalverwaltungen und Mitarbeitern hat in den letzten Jahren zu einer Vielzahl klärungsbedürftiger Fragen geführt. Die Bundesregierung wird sich hiermit im einzelnen befassen. Sie sieht es jedoch als unmöglich an, alle Einzelfälle expressis verbis gesetzlich zu regeln. Dies würde dem Grundsatz der Rechtsvereinfachung widersprechen. Daher wird eine gesetzliche Neuordnung des Personalaktenrechts generalklauselartige Aussagen nicht vermeiden können. Eine überladene Kasuistik würde den Rechtsschutz eher mindern als stärken.

Klärungs- bzw. regelungsbedürftig sind nach dem gegenwärtigen Stand der Überlegungen folgende Problembereiche:

— Befugnis zur Führung von Personalakten

Die Befugnis und Pflicht zur Führung von Personalakten wurde bisher entsprechend früherer Gesetzgebungstechnik in den § 90 BBG, § 56 BRRG vorausgesetzt. Eine ausdrückliche Vorschrift, daß über jeden Beamten Personalakten zu führen sind, erscheint rechtssystematisch sinnvoll.

— Inhalt der Personalakten

Der notwendige Inhalt der Personalakten ist festzulegen. Dabei soll — auch im Sinne der höchstrichterlichen Rechtsprechung — klargestellt werden, daß die betreffenden Vorgänge in einem inneren Zusammenhang mit dem Beamtenverhältnis stehen müssen. Außerdem wird der Zweckbindungsgrundsatz zu betonen sein. Ausnahmen von diesem Grundsatz sind gesetzlich festzulegen.

In diesem Zusammenhang wird u. a. auch geregelt werden

— Behandlung von Bewerbungsunterlagen einschl. der Vorakten (z. B. Prüfungsakten, Referendarakten)

— Inhalt und Behandlung von Personalbögen

— Inhalt und Behandlung von sensiblen Vorgängen wie z. B. personalärztlichen Unterlagen.

Gehören Vorgänge zum notwendigen Inhalt der Personalakte, können sie nur entfernt (bzw. gelöscht) werden, wenn dazu eine Ermächtigung vorliegt. Der Inhalt der Ermächtigung ist festzulegen (z. B. bei unbegründeten Beschwerden, falschen Behauptungen). Die Regelungen der §§ 49, 50 Bundeszentralregistergesetz sind in die Überlegungen miteinzubeziehen.

— Personalaktengeheimnis

Die gesetzliche Verankerung des Personalaktengeheimnisses ist eine Selbstverständlichkeit, ebenso das Recht des Beamten auf uneingeschränkte Einsicht in seine Personalakte. Für Ausnahmen von dieser Grundregel bedarf es einer gesetzlichen Ermächtigung, die unter Beachtung des Grundsatzes der Verhältnismäßigkeit in dem Umfang gewährt werden kann, als die Einsicht zur Erfüllung gesetzlicher Aufgaben oder im überwiegenden dienstlichen oder öffentlichen Interesse zwingend geboten ist. Gleiches sollte für Auskünfte aus den Personalakten sowie für deren Weitergabe gelten. Der Sicherung des Personalaktengeheimnisses können auch organisatorische Regelungen dienen, z. B. die besondere aktenmäßige Behandlung hochsensibler wie z. B. ärztlicher Unterlagen oder die sog. aktenmäßige Abschottung von Teilen der Personalakte, wie dies anhand der Beihilfeakten besonders intensiv diskutiert worden ist und bei der Neufassung der Allgemeinen Verwaltungsvorschrift über die Gewährung von Beihilfen in Krankheits-, Geburts- und Todesfällen vom 19. April 1985 (GMBl. 1985, S. 290ff.) bereits Berücksichtigung gefunden hat.

— Personalinformationssysteme

Die Bundesregierung hat in der Beantwortung der Großen Anfrage der Fraktion der SPD vom 10. Dezember 1985 (Drucksache 10/4594) ausführlich zu den spezifischen Problemen von Personalinformationssystemen Stellung bezogen. Die Bundesregierung hat sich dazu bekannt, keine Personalinformationssysteme einzuführen, die die gesamte Persönlichkeit des Beschäftigten umfassen oder die durch die Verknüpfung mit anderen Datensammlungen zu sensiblen Informationsträgern werden. Aus diesem Grunde wird die Bezeichnung „automatisierte Personalverwaltungssysteme" für zweckmäßiger gehalten. Mit ihnen wird lediglich der Zweck verfolgt, die Personalverwaltung von umfangreichen, fehlerträchtigen und arbeitsintensiven manuellen Tätigkeiten zu entlasten. An die Erstellung und Erfassung von Persönlichkeitsprofilen ist nicht gedacht.

Automatisierte Personalverwaltungssysteme werden auch in Zukunft nur Entscheidungshilfen für Perso-

nalentscheidungen sein; die Entscheidung selbst wird nicht dem System überlassen werden. Insoweit besteht Übereinstimmung mit dem Bundesbeauftragten für den Datenschutz.

Die Bundesregierung wird im Rahmen der Neuordnung des Personalaktenrechts prüfen, welche bereichsspezifischen gesetzlichen Regelungen datenschutzrechtlicher Art neben den zu schaffenden allgemeinen Bestimmungen des Personalaktenrechts notwendig sind, um bei Verarbeitung personenbezogener Daten von Angehörigen des öffentlichen Dienstes im Rahmen der Zweckbestimmung des Dienstverhältnisses eine größtmögliche Sicherung der Persönlichkeitsrechte zu erreichen.

In diesem Zusammenhang wird auch zu prüfen sein, welche verfahrensmäßigen und sicherungstechnischen Vorkehrungen — insbesondere beim Einsatz von Arbeitsplatzrechnern — zu treffen sind, um auch technisch-organisatorisch den Datenschutz sicherzustellen.

— Verwaltung und Führung von Personalakten

Die ordnungsgemäße Personalaktenführung ist, insbesondere wegen der erhöhten Sicherungsmaßnahmen, personalaufwendig. Hinzu kommt wegen der teilweise langen Aufbewahrungszeit ein erheblicher Lagerraumbedarf. Nach Erfahrungswerten des Bundesrechnungshofes werden für die Aufbewahrung der Personal- und Versorgungsakten für je 100 000 Beschäftigte Regale in der Länge von rd. 10 km erforderlich. Diese Werte machen deutlich, welche wirtschaftliche Tragweite Bemühungen um Verringerung des Personalaktenbestandes haben.

Folgende Maßnahmen sind eingeleitet worden:

- Vereinheitlichung der Vorschriften für das Führen und Verwalten von Personalakten mit dem Ziel einer klaren Gliederung in der Aktenführung und der organisatorischen Umsetzung der einschlägigen gesetzlichen Schutzvorschriften.
- Verringerung des Lagerraums durch Mikroverfilmung. Pilotuntersuchungen mit den verschiedenen technischen Verfahren sind abgeschlossen bzw. eingeleitet.
- Festlegung von Aufbewahrungsfristen für die Hauptpersonalakte und einzelner Teile der Personalakte.
- Festlegung der personalaktenführenden Stelle.

Weitere Maßnahmen werden geplant.

III.

Die Bundesregierung hat für die geschilderten Planungs- und Prüfungsarbeiten eine interministerielle Arbeitsgruppe beim Bundesminister des Innern eingesetzt. Sie wird bemüht sein, möglichst bald realisierungsfähige Vorschläge vorzulegen. Der Abschluß der Arbeiten hängt jedoch u. a. auch von dem Gang der notwendigen Beteiligungsgespräche ab.

Zu 5.1. Konventionelle Personaldatenverarbeitung

Zu 5.1.1. Beihilfe

Der Bundesbeauftragte für den Datenschutz begrüßt die in § 17 Abs. 4 der Beihilfevorschriften des Bundes getroffene Regelung über die vertrauliche Behandlung von Beihilfedaten.

Die vom Bundesbeauftragten für den Datenschutz geforderte besondere Verschwiegenheitspflicht des Beihilfesachbearbeiters auch gegenüber seinem Vorgesetzten kann nach Auffassung der Bundesregierung nicht weitergehen als im Sozialrecht. In § 35 des Ersten Buches Sozialgesetzbuch kommt zum Ausdruck, daß die aufsichts-, rechnungsprüfungs- und weisungsberechtigten Behörden im Rahmen des § 69 Abs. 1 Nr. 1 SGB X Kenntnis vom Sozialgeheimnis des Versicherten nehmen dürfen. Entsprechendes gilt auch für die Stellen in der Behördenorganisation, die gegenüber dem Beihilfesachbearbeiter aufsichts-, rechnungsprüfungs- und weisungsberechtigt sind. Beispielsweise muß der Vorgesetzte des Beihilfesachbearbeiters Kenntnis vom Sachverhalt nehmen können, wenn ein Widerspruchsbescheid zu erteilen ist.

Soweit diese Einschränkungen nicht gelten, folgt die Schweigepflicht des Beihilfesachbearbeiters gegenüber anderen Bediensteten schon aus § 61 BBG bzw. § 9 BAT sowie insbesondere aus § 17 Abs. 4 der Allgemeinen Verwaltungsvorschrift über die Gewährung von Beihilfe in Krankheits-, Geburts- und Sterbefällen. Die vom Bundesbeauftragten für den Datenschutz für Beihilfesachbearbeiter angeregte besondere förmliche Verpflichtung zur Verschwiegenheit wird von der Bundesregierung nicht für erforderlich gehalten.

Für bedenklich hält der Bundesbeauftragte für den Datenschutz, daß bei der Bundesversicherungsanstalt für Angestellte dieselben Bearbeiter für Beihilfesachen und allgemeine Personalangelegenheiten zuständig sind.

Nach Mitteilung des Bundesministers für Arbeit und Sozialordnung ist bei der Bundesversicherungsanstalt für Angestellte vorgesehen, entsprechend den Wünschen des Bundesbeauftragten für den Datenschutz, die Beihilfe von der übrigen Personalsachbearbeitung zu trennen. Hierzu bedarf es jedoch der Klärung einer Reihe organisatorischer Fragen mit möglichen Auswirkungen auf den Stellenplan. Die Bundesversicherungsanstalt für Angestellte ist bemüht, die Trennung gleichwohl alsbald zu realisieren.

Zu 5.1.2. Umgang mit ärztlichen Unterlagen

Der Bundesbeauftragte für den Datenschutz ist der Meinung, daß die Behandlung ärztlicher Unterlagen im Personalwesen bei der Bundesversicherungsanstalt für Angestellte nicht den datenschutzrechtlichen Anforderungen entspricht.

Diese Aussage ist so wenig konkret, daß eine Stellungnahme dazu nicht möglich ist. Im übrigen handelt es sich bei den ärztlichen Unterlagen nicht um Dateien.

Des weiteren stellt der Bundesbeauftragte für den Datenschutz seine Auffassung über die Behandlung ärztlicher Gutachten und Zeugnisse im Zusammenhang mit Entscheidungen über die Verwendung von Bediensteten und der ärztlichen Überprüfung von Beihilfeangelegenheiten klar.

Die Bundesregierung begrüßt diese Klarstellung, unbeschadet der Tatsache, daß es sich auch insoweit nicht um die Verarbeitung von Daten in Dateien handelt. Nach den im Tätigkeitsbericht aufgestellten Grundsätzen wird allgemein in der Bundesverwaltung verfahren.

Zu 5.1.3. Einzelfälle

— Der Bundesbeauftragte für den Datenschutz bemängelt, daß Übersichten mit personenbezogenen Daten von Bediensteten, die die Auswahlentscheidung bei Stellenbesetzungen erleichtern und rechtfertigen sollen, nicht bei den formellen Personalakten geführt werden und nicht dem Einsichtsrecht des Betroffenen unterliegen.

  Der Bundesminister für Arbeit und Sozialordnung vertritt hierzu die Auffassung, daß nach dem arbeitsrechtlichen Schrifttum solche Übersichten durchaus dem materiellen Personalaktenbegriff, aber nicht dem Einsichtsrecht unterliegen, wenn die betreffenden Daten nicht anonymisiert werden können und die anderen Arbeitnehmer nicht auf die Vertraulichkeit ihrer Daten verzichten (vgl. BVerwG MDR 76, 78; Hümmerich/Gola, Personaldatenrecht im Arbeitsverhältnis, Heidelberg 1975, S. 108; Fitting-Auffahrt-Kaiser, zu § 83 BetrVerfG, Rdnr. 17).

  Dem einzelnen Arbeitnehmer kann nicht Einsicht gewährt werden, wenn damit zugleich Personaldaten anderer Mitarbeiter offenbart würden und so deren informationelles Selbstbestimmungsrecht verletzt würde.

— Der Bundesbeauftragte für den Datenschutz spricht sich für eine Änderung des Verfahrens bei der Angabe von Urlaubsanschriften dergestalt aus, diese nicht im Urlaubsantrag aufzuführen sind, sondern dem direkten Vorgesetzten mitgeteilt werden.

  Die Bundesregierung hält auch bei kritischer Abwägung der gegensätzlichen Interessen einen Verzicht auf die Angabe der Urlaubsanschrift auf dem Urlaubsantrag für nicht möglich.

  Der Widerruf von Erholungsurlaub ist aus dienstlichen Gründen jederzeit zulässig. Wenn von diesem Recht Gebrauch gemacht wird, ist es im allgemeinen besonders wichtig, die Dienstbereitschaft schnell herzustellen. Schon dieser Gesichtspunkt verbietet die Angabe von Kontaktadressen o. ä. Zusätzlich sprechen Gründe der Arbeitsökonomie gegen die Änderung des bisherigen Verfahrens, da aufwendige Nachforschungen notwendig werden, wenn der „Kontaktmann" nicht erreichbar ist.

  Dagegen ist durch die Angabe der Urlaubsanschrift auf dem Urlaubsantrag sichergestellt, daß im Personalreferat jederzeit Auskunft über den Aufenthaltsort von Mitarbeitern gegeben werden kann. Die für alle persönlichen Daten geltende Vertraulichkeit wird dabei selbstverständlich gewahrt.

Zu 5.2. *Automatisierte Personaldatenverarbeitung*

Zu 5.2.4. Mitbestimmung und bereichsspezifische gesetzliche Regelung des Arbeitnehmerdatenschutzes

Die Bundesregierung wird den Entwurf einer bereichsspezifischen Regelung des Arbeitnehmerdatenschutzes so bald wie möglich in der nächsten Legislaturperiode dem Deutschen Bundestag vorlegen. Ihre Überlegungen zur inhaltlichen Ausgestaltung hat die Bundesregierung in der Beantwortung der Großen Anfrage der Fraktion der SPD zu Personalinformationssystemen und Datenschutz vom 19. Dezember 1985 (Drucksache 10/4594) dargelegt. Die Empfehlungen des Bundesbeauftragten für den Datenschutz für dieses Vorhaben wird sie in ihre Überlegungen einbeziehen.

Zu 6. Deutsche Bundespost

Der Bundesminister für das Post- und Fernmeldewesen bemerkt zu den Prüfungsfeststellungen des Bundesbeauftragten für den Datenschutz, daß wie im Vorjahr auch im Berichtsjahr 1985 keine förmliche Beanstandung gemäß § 20 Abs. 1 BDSG ausgesprochen worden ist. Im Hinblick auf die vielfältigen datenschutzrechtlich bedeutsamen Tätigkeiten der Deutschen Bundespost — vorwiegend im Rahmen der Einführung neuer Kommunikationstechniken — ergeben sich für den Bundesbeauftragten für den Datenschutz aus der Sicht des Datenschutzes jedoch mannigfaltige Fragen nach der Erforderlichkeit und somit der Zulässigkeit der eingesetzten Verfahren sowohl aus Anlaß der Durchführung von Beratungen und datenschutzrechtlichen Kontrollen als auch aufgrund entsprechender an ihn gerichteter Eingaben der Bürger. Über die bereichsspezifischen Anforderungen des Datenschutzes — insbesondere im Zusammenhang mit der Einführung neuer Dienstleistungen — führt der Bundesbeauftragte für den Datenschutz eine permanente und teilweise kontroverse Diskussion mit der Deutschen Bundespost.

Vor diesem Hintergrund geht der Bundesbeauftragte für den Datenschutz zum einen auf Einzelfälle ein, die im Berichtsjahr Gegenstand von Erörterungen und Kontrollen waren, zum anderen spricht er Themen von grundsätzlicher Bedeutung an.

Der Bundesminister für das Post- und Fernmeldewesen bedauert im übrigen, daß die Deutsche Bundespost im Rahmen der Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz keine Möglichkeit hatte, sich zu allen im Tätigkeitsbericht getroffenen Feststellungen und Anregungen vor dessen Ver-

öffentlichung zu äußern. Im Hinblick auf die große Publizität, die die Tätigkeitsberichte des Bundesbeauftragten für den Datenschutz genießen, und im Interesse der Öffentlichkeit an umfassender Information sollte der Bundesbeauftragte für den Datenschutz prüfen, ob das Verfahren des Bundesrechnungshofes übernommen werden kann. Der Bundesrechnungshof gibt den Entwurf seines Prüfberichts dem jeweils zuständigen Minister zur Stellungnahme. Im Prüfbericht berichtet er dann über seine Feststellungen, die Auffassung der Verwaltung und seine abschließende Bewertung. Ein solches Verfahren würde dem Leser der Tätigkeitsberichte bei kontrovers diskutierten Sachverhalten beide Ansichten gleichzeitig zur Kenntnis bringen und damit zu einer objektiven, ausgewogenen Information beitragen.

Zu 6.1. Zusammenarbeit mit dem Bundesminister für das Post- und Fernmeldewesen

Der Bundesbeauftragte für den Datenschutz sieht die Effektivität der Zusammenarbeit mit der Deutschen Bundespost dadurch beeinträchtigt, daß er nicht frühzeitig über geplante Dienste bzw. Techniken informiert würde, die Deutsche Bundespost ihm entgegenhalte, personenbezogene Daten würden nicht in Dateien gespeichert und die Bearbeitungsdauer beim Bundesminister für das Post- und Fernmeldewesen gelegentlich unverhältnismäßig lang sei.

Nach der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkt 6.2.2) soll dem Bundesbeauftragten für den Datenschutz bei der Einführung neuer DV-gestützter Dienste nach Möglichkeit frühzeitig Gelegenheit gegeben werden, Empfehlungen zur Gewährleistung des Datenschutzes zu geben.

Der Bundesminister für das Post- und Fernmeldewesen führt hierzu aus:

Die Deutsche Bundespost ist bemüht, den Bundesbeauftragten für den Datenschutz nicht erst bei Einführung neuer oder bei der technisch-betrieblichen Umgestaltung schon bestehender Fernmeldedienste, bei denen personenbezogene Daten verarbeitet werden, zu unterrichten. Die Deutsche Bundespost informiert den Bundesbeauftragten für den Datenschutz bei datenschutzmäßig wesentlichen Vorgängen möglichst schon im Planungsstadium, wenn die beabsichtigten Neuerungen hinreichend konkretisiert sind. Im übrigen weist der Bundesminister für das Post- und Fernmeldewesen darauf hin, daß die datenschutzmäßige Verantwortung bei der datenverarbeitenden Verwaltung liegt und eine Pflicht zur ausnahmslosen Beteiligung des Bundesbeauftragten für den Datenschutz nicht besteht. Vielmehr liegt es im Ermessen der allein datenschutzmäßig verantwortlichen Verwaltung, im Einzelfall zu entscheiden, ob eine Beratung durch den Bundesbeauftragten für den Datenschutz angezeigt ist. Damit wird auch dem Interesse des Bundesbeauftragten für den Datenschutz, nur in wesentlichen Fragen beteiligt zu werden, Rechnung getragen, ohne daß das Prüfungsrecht des Bundesbeauftragten für den Datenschutz hierdurch abgeschwächt wird.

Der Bundesminister für das Post- und Fernmeldewesen hält an seiner Rechtsauffassung fest, daß der Bundesbeauftragte für den Datenschutz, wenn er die Einhaltung von Vorschriften des BDSG oder anderer Rechtsvorschriften über den Datenschutz kontrolliert, an die in § 1 Abs. 2 Satz 1 bestimmten Grenzen des sachlichen Anwendungsbereiches des BDSG gebunden ist. Es ist in das Ermessen der Deutschen Bundespost gestellt, ob sie eine Beratung durch den Bundesbeauftragten für den Datenschutz in Anspruch nehmen will. Dabei wird auch zu berücksichtigen sein, ob der Bundesbeauftragte für den Datenschutz für den jeweiligen Regelungssachverhalt im Sinne der vorstehenden Ausführungen sachlich zuständig ist.

Die Deutsche Bundespost hat einen dreistufigen Behördenaufbau (Amtsebene, Direktionsebene und Ministerium). Dies führt dazu, daß oftmals Rückfragen des Bundesministers für das Post- und Fernmeldewesen bei betroffenen nachgeordneten Behörden zur Ermittlung des zutreffenden Sachverhaltes erforderlich sind. In Einzelfällen kann dies zu Zeitverzögerungen führen. Der Bundesminister für das Post- und Fernmeldewesen ist jedoch bemüht, die Bearbeitungszeiten der einzelnen Vorgänge in einem vertretbaren Zeitrahmen zu halten. Entsprechend dem Vorschlag des Bundesbeauftragten für den Datenschutz wird künftig vermehrt von der Möglichkeit, Teilbescheide zu erteilen, Gebrauch gemacht.

Zu 6.2. Bildschirmtext

In der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkt 6.4) wird die Bundesregierung gebeten zu prüfen, ob und inwieweit die vorhandenen bereichsspezifischen Datenschutzregelungen für das Bildschirmtext-System ergänzungsbedürftig sind.

Die Prüfung dieser Frage durch den Bundesminister für das Post- und Fernmeldewesen hat folgendes ergeben:

Die Deutsche Bundespost steht nach wie vor auf dem Standpunkt, daß keine rechtliche Verpflichtung besteht, alle datenschutzmäßig relevanten Umstände des Bildschirmtextdienstes durch bereichsspezifische Vorschriften zu regeln. Weder verpflichtet das BDSG hierzu noch läßt sich eine solche Verpflichtung aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz herleiten. Da die Teilnehmer freiwillig an den Diensten der Deutschen Bundespost teilnehmen, werden ihnen personenbezogene Daten nicht zwangsweise abverlangt, so daß kein Eingriff des Staates in Grundrechtspositionen gegeben ist, der eine detaillierte, bereichsspezifische Regelung erforderlich machen würde.

Die Deutsche Bundespost hat jedoch aus Zweckmäßigkeitsgründen den Entwurf einer „Verordnung über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Fernmeldewesens (Tele-

kommunikationsordnung — TKO)" zum Anlaß genommen, die bisher vorhandenen Regelungen unter weitgehender Berücksichtigung der Vorstellungen des Bundesbeauftragten für den Datenschutz zu überarbeiten und zu ergänzen. Der Entwurf der TKO enthält einen eigenständigen Abschnitt, in welchen allgemeine Datenschutzvorschriften für alle Telekommunikationsdienste (§§ 382 bis 386 TKO) sowie zusätzliche Bestimmungen, u. a. für den Datenschutz im Bildschirmtextdienst (§ 387 TKO), aufgenommen wurden.

Zu den Bemühungen der Deutschen Bundespost um Zugangssicherung zum Bildschirmtext-Dienst, wie es dem erhofften Massenbetrieb angemessen ist, ist zu bemerken:

Die Deutsche Bundespost hat die technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um den Benutzerzugang zum Bildschirmtext-Dienst zu sichern. Sie unternimmt in Anwendung des § 6 Abs. 1 BDSG alle Anstrengungen, um die Sicherheit des Benutzerzugangs so zu erhöhen, wie das dem angestrebten „Massenverkehr" angemessen ist. Mit der Entwicklung und der Einführung der Chipkarte in den nächsten Jahren wird die Zugangssicherheit noch weiter verbessert werden können.

Zur Frage, inwieweit gesetzliche Beschränkungen des Fernmeldegeheimnisses — namentlich nach dem Gesetz zu Artikel 10 GG (G 10) — auch für Btx gelten, nimmt der Bundesminister für das Post- und Fernmeldewesen wie folgt Stellung:

Grundsätzlich wird das Fernmeldegeheimnis durch die Aufnahme (Registrierung) und Weitergabe (Bekanntgabe) sowohl des Inhalts der Nachricht als auch der näheren Umstände der Übermittlung, die sog. Fernmeldeverbindungsdaten, betroffen. Soweit bei Btx Text und grafische Darstellungen allgemein zugänglich und nicht durch einen Abruf zu einer bestimmten Person in Beziehung zu setzen sind, unterliegen diese nicht dem Fernmeldegeheimnis. Ebensowenig wird das Fernmeldegeheimnis durch die bei Btx anfallende Registrierung von Vergütungsdaten, die auch Aussagen zu Fernmeldeverkehrsbeziehungen zwischen Teilnehmern, d. h. über nähere Umstände des Fernmeldeverkehrs enthalten, eingeschränkt. In die Registrierung der Vergütungsdaten willigt der Anbieter mit der Wirkung ein, daß das Fernmeldegeheimnis von vornherein nicht berührt wird. In allen anderen Fällen werden der konkret übermittelte Nachrichteninhalt und die Umstände des konkreten Btx-Verkehrs vom Fernmeldegeheimnis erfaßt.

Gemäß § 12 Fernmeldeanlagengesetz (FAG) können in strafgerichtlichen Untersuchungen der Richter und — bei Gefahr im Verzug — auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und daß die Auskunft für die Untersuchung Bedeutung hat.

Auskünfte über Btx-Verkehr, der dem Fernmeldegeheimnis unterliegt, können danach nur insoweit gegeben werden, als dieser festgehalten wird. Dies trifft bei Btx nur für die Vergütungsdaten zu, aus denen auf Fernmeldeverkehrsbeziehungen zwischen Btx-Teilnehmern, grundsätzlich jedoch nicht auf den Abruf einer bestimmten Information einer Seite des Btx-Dienstes (Nachrichteninhalt) geschlossen werden kann. Die Beschränkung des Fernmeldegeheimnisses durch § 12 FAG bezieht sich somit auf die Bekanntgabe der angefallenen Vergütungsdaten.

Die Bundesregierung ist der Auffassung, daß Btx rechtlich als Fernmeldeverkehr zu qualifizieren ist. Btx-Nachrichtenaustausch vollzieht sich fernmeldemäßig i. S. von § 1 Fernmeldeanlagengesetz. Der Verkehr wird drahtgebunden im Fernsprechnetz der Deutschen Bundespost abgewickelt und unterscheidet sich von anderen Fernmeldediensten nur in seiner Erscheinungsform. Als im Fernmeldewesen abgewickelter Nachrichtenverkehr genießt Btx damit auch den Schutz des Fernmeldegeheimnisses nach Artikel 10 GG. § 1 Abs. 1 G 10 stellt auf das Abhören und Aufnehmen von Fernmeldeverkehr ab. Die Materialien zum G 10 sprechen dafür, daß der Gesetzgeber — auch wenn er sich an den damals gegebenen technischen Möglichkeiten orientierte — keine abschließende Aufzählung der Möglichkeiten vornehmen wollte. Die Rechtsauffassung der Bundesregierung wird vom Gremium nach Artikel 10 GG geteilt.

Zur Auffassung des Deutschen Bundestages, daß zur Wahrnehmung der jeweiligen Prüfungskompetenz des Bundesbeauftragten für den Datenschutz und der Landesbeauftragten für den Datenschutz die Auskunftserteilung der Deutschen Bundespost geregelt werden müsse, bemerkt der Bundesminister für das Post- und Fernmeldewesen:

Die Deutsche Bundespost ist nicht der Auffassung, daß es zusätzlicher Regelungen für die Erteilung von Auskünften der Deutschen Bundespost über den Btx-Dienst an den Bundesbeauftragten für den Datenschutz sowie die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden der Länder bedarf. Der Bildschirmtextdienst ist ein benutzungsrechtlich geregelter Fernmeldedienst. Er dient der körperlosen Übermittlung von Nachrichten in Form von Texten und grafischen Darstellungen und zählt damit zum Fernmeldewesen. Im Rahmen des Btx-Dienstes werden personenbezogene Daten der Teilnehmer von den Fernmeldeämtern gespeichert. Für die Kontrolle der Einhaltung der Vorschriften des BDSG ist daher der Bundesbeauftragte für den Datenschutz zuständig (§ 19 Abs. 1, § 7 Abs. 1 BDSG). Die Deutsche Bundespost erfüllt die in § 19 Abs. 3 BDSG verankerte Verpflichtung, den Bundesbeauftragten für den Datenschutz und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen, indem sie ihnen insbesondere Auskunft zu Fragen gibt und Zutritt zu den Diensträumen gewährt.

Die datenschutzmäßige Kontrolle des „Nutzungsbereichs" ist Aufgabe der Landesbehörden. Für die Kontrolle des öffentlich-rechtlichen Bereichs, d. h. im wesentlichen die Landes- und Kommunalbehörden und die der Aufsicht des Landes unterliegenden juristischen Personen des öffentlichen Rechts, ist der Landesdatenschutzbeauftragte zuständig. Die Datenverarbeitung nichtöffentlicher Stellen wird durch die

nach Landesrecht zuständigen Aufsichtsbehörden (§§ 30, 40 BDSG) überwacht.

Die Deutsche Bundespost erteilt den Landesdatenschutzbeauftragten und den Aufsichtsbehörden der Länder Auskünfte über den Btx-Dienst, soweit sie diese zur Erfüllung der ihnen obliegenden Aufgaben benötigen. So fand beispielsweise am 8. November 1984 eine eingehende Besprechung mit den Datenschutzbeauftragten des Bundes und der Länder über technische und rechtliche Fragen des Bildschirmtextdienstes statt. Darüber hinaus unterstützt die Deutsche Bundespost die Datenschutzbehörden der Länder bei der Erledigung von Einzelfällen im Wege der Amtshilfe. Dieses Verfahren hat sich in der Praxis bewährt.

Zu 6.2.2. Kontrollkompetenz; Regelungsdefizite

Der Bundesbeauftragte für den Datenschutz hält die Zugangssicherung bei Bildschirmtext (Btx) zur Verhinderung eines unbefugten Systemzuganges durch sogenannte „Hacker" — es wird der Fall eines unbefugten Abrufs entgeltpflichtiger Seiten einer Sparkasse durch Mitglieder eines Computer-Clubs im Wege der Identitätstäuschung angesprochen — für noch nicht ausreichend gewährleistet. Außerdem wird die mangelnde Normenklarheit bei Btx von ihm als unbefriedigend empfunden.

Der Bundesminister für das Post- und Fernmeldewesen bemerkt hierzu, daß die technischen Prüfungen der Deutschen Bundespost ergeben haben, daß die Kennung des Btx-Anschlusses der im Bericht angesprochenen Sparkasse nicht durch einen Fehler im Btx-System bekanntgeworden sein kann, sondern vermutlich auf zu sorglosem Umgang des Kreditinstituts mit dem geheimen Kennwort bei Btx-Demonstrationen zurückzuführen ist.

Hinsichtlich der Auffassung des Bundesbeauftragten für den Datenschutz, die mangelnde Normenklarheit bei Btx sei unbefriedigend, wird auf die Ausführungen zu Punkt 6.4 Abs. 1 in der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz verwiesen. Danach wird die von der Deutschen Bundespost im Entwurf einer Telekommunikationsordnung (TKO) konzipierte datenschutzrechtliche Regelung auch den besonderen Vorstellungen des Bundesbeauftragten für den Datenschutz über Normenklarheit und Transparenz gerecht.

Der Bundesbeauftragte für den Datenschutz stellt im Hinblick auf den Erlaß einer Benutzungsverordnung wie der TKO die grundsätzliche Frage nach der Tragfähigkeit der Verordnungsermächtigung des § 14 Postverwaltungsgesetz (PostVwG) für die Einführung und Regelung neuer technischer Kommunikationsdienste durch den Bundesminister für das Post- und Fernmeldewesen. Diese Frage nach der Regelungsbefugnis wiederholt der Bundesbeauftragte für den Datenschutz auch in den Ausführungen zu Temex (6.3.3) und zum Elektronischen Telefonbuch (6.4.2). Diesbezüglichen Zweifel stützt der Bundesbeauftragte für den Datenschutz auf die vom Bundesverfassungsgericht entwickelte Wesentlichkeitstheorie, wonach der Gesetzgeber in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, alle wesentlichen Entscheidungen selbst zu treffen hat (s. a. BVerfGE 49 Seite 126).

Nach Auffassung des Bundesministers für das Post- und Fernmeldewesen stellt § 14 PostVwG eine ausreichende Rechtsgrundlage für die Einführung und Regelung neuer technischer Kommunikationsdienste dar.

Vorgänge und Regelungen dieser Art sind weniger unter dem Aspekt der eher unbestimmten Wesentlichkeitstheorie zu werten. Das Bundesverfassungsgericht wendet diese Theorie im Bereich von Ermächtigungen zum unmittelbaren Verwaltungshandeln (z. B. Verwaltungsanweisungen, Verwaltungsakte) an. Bei der Ermächtigung der Verwaltung zur abstrakten Rechtsetzung (Erlaß von Rechtsverordnungen) stellt das Bundesverfassungsgericht auf Artikel 80 Abs. 1 Satz 2 Grundgesetz ab. Es sieht in dieser Verfassungsnorm eine konkrete Ausformung der Wesentlichkeitstheorie.

Bei der Prüfung, ob § 14 PostVwG in diesem Sinn verfassungskonform ist, kann auf die gefestigte und ständige Rechtsprechung des Bundesverfassungsgerichts zur Bestimmtheit von Ermächtigungsnormen zurückgegriffen werden. Danach wird nicht gefordert, daß die Ermächtigungsnorm als isolierte Vorschrift in sich schon hinreichend bestimmt sein muß. Es genügt, wenn der Gesetzgeber mit der Ermächtigungsnorm im Zusammenhang mit anderen Vorschriften des Gesetzes und der Zielsetzung des Gesetzes insgesamt dem Verordnungsgeber ein Programm vorgegeben und so die Grenzen abgesteckt hat. Dabei dürfen im Bereich der Leistungsverwaltung die Anforderungen an die Bestimmtheit geringer sein als im Bereich der Eingriffsverwaltung.

Aus § 14 PostVwG in Verbindung mit § 2 PostVwG — Bindung an die vielfach gesetzlich festgelegten Grundsätze der Politik, Bindung an die Interessen der Volkswirtschaft, Verpflichtung zur Entwicklung der Post- und Fernmeldedienste und der technischen Anlagen — ist ein hinreichend deutliches Programm für den Verordnungsgeber abzuleiten.

Zu 6.4. Eintrag der Teilnehmer ins Telefonbuch

Zu 6.4.1. „Zwangseintragung"

Nach Auffassung des Bundesbeauftragten für den Datenschutz muß die Zulässigkeit der Vorschriften über die „Zwangseintragung" im Telefonbuch (§ 39 Abs. 2 Satz 1 Fernmeldeordnung) daraufhin geprüft werden, ob die durch sie bestimmte Einschränkung des Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse liegt.

Der Bundesminister für das Post- und Fernmeldewesen bedauert, daß der Bundesbeauftragte für den Datenschutz die Eintragung der Teilnehmer im amtlichen Fernsprechbuch im Gegensatz zu früheren Tätigkeitsberichten nun als „Zwangseintragung" be-

zeichnet. Die Eintragung der Teilnehmer in das amtliche Fernsprechbuch ist eine benutzungsrechtlich vorgeschriebene Bedingung der Teilnahme am Telefondienst der Deutschen Bundespost. Da die Teilnehmer zu den Bedingungen der Fernmeldeordnung freiwillig am Fernsprechdienst teilnehmen, werden die Daten nicht zwangsweise erhoben, so daß mit der Eintragung nicht zwangsweise in das Persönlichkeitsrecht der einzelnen eingegriffen wird. Außerdem liegt es im überwiegenden Allgemeininteresse, daß die Teilnehmer am Fernsprechdienst im Teilnehmerverzeichnis eingetragen sind, da nur so ein reibungsloser Fernsprechverkehr zu ermöglichen ist. Durch die großzügige Anerkennung von Gründen für Nichteintragungen und durch Kurzeinträge werden die Interessen der Teilnehmer ausreichend berücksichtigt. Auch die Gerichte haben die durch § 39 Abs. 2 Fernmeldeordnung getroffenen Regelungen als gesetzes- und verfassungskonform anerkannt.

Zu 6.4.2. Elektronisches Telefonbuch

Der Bundesbeauftragte für den Datenschutz äußert die Besorgnis, mit Hilfe des elektronischen Telefonbuchs (ETB) könnte mit relativ geringem Aufwand der Aufenthaltsort eines Fernsprechteilnehmers bundesweit ermittelt werden. Das ETB würde damit angesichts der hohen Telefondichte einem Bundesadreßregister nahekommen.

Der Bundesminister für das Post- und Fernmeldewesen bemerkt hierzu:

Es muß das Bestreben einer modernen Fernmeldeverwaltung sein, den Teilnehmern und Benutzern aktuelle Auskunftsmöglichkeiten zur reibungslosen Abwicklung des Gesprächsverkehrs zur Verfügung zu stellen. Die Deutsche Bundespost teilt die Besorgnis des Bundesbeauftragten für den Datenschutz nicht, daß mit Hilfe des elektronischen Telefonbuchs mit relativ geringem Aufwand der Aufenthaltsort eines Fernsprechteilnehmers bundesweit ermittelt werden könnte, was angesichts der hohen Telefondichte in der Bundesrepublik Deutschland einem Bundesadreßregister nahekäme. Die technischen Eigenschaften des elektronischen Telefonbuchs sind so ausgestaltet, daß sein Inhalt nicht leichter ausgewertet werden und kopiert werden kann als der der gedruckten Telefonbücher. Das gilt auch für die Auswertbarkeit der in den Telefonbüchern enthaltenen Adressen zu Werbezwecken.

Zur Frage der Eintragung der Teilnehmer in das elektronische Telefonbuch unter dem Aspekt des informationellen Selbstbestimmungsrechts wird auf die Antworten der Bundesregierung vom 2. Oktober 1985 und 30. Oktober 1985 auf Kleine Anfragen der Abgeordneten Frau Dann und der Fraktion DIE GRÜNEN verwiesen (Drucksachen 10/3934 und 10/4112). Das informationelle Selbstbestimmungsrecht steht einer Eintragung der Teilnehmer nicht entgegen. Die Teilnehmer nehmen zu den Bedingungen der Fernmeldeordnung freiwillig am Fernsprechdienst teil. Die Daten werden daher nicht zwangsweise erhoben, so daß mit der Eintragung nicht zwangsweise in das Persönlichkeitsrecht der Teilnehmer eingegriffen wird. Außerdem sind die Daten ohnehin zur Veröffentlichung im amtlichen Fernsprechbuch vorgesehen und über die Fernsprechauskunft jedermann zugänglich.

Das elektronische Telefonbuch wird von der Deutschen Postreklame GmbH in Zusammenarbeit mit örtlichen Verlegern herausgegeben. Die Deutsche Postreklame GmbH und nicht die Deutsche Bundespost ist daher speichernde Stelle im Sinne des Bundesdatenschutzgesetzes. Zur datenschutzrechtlichen Kontrolle ist daher die hessische Aufsichtsbehörde zuständig (§ 30 BDSG), die von der Deutschen Postreklame GmbH auch schon Auskünfte eingeholt und mit ihr Gespräche geführt hat.

Zu 6.5. Fernsprechauskunft

Die Deutsche Bundespost teilt die Auffassung des Bundesbeauftragten für den Datenschutz, daß Datenschutzgründe der Bekanntgabe der Wohnungsanschrift eines Teilnehmers, die im amtlichen Fernsprechbuch eingetragen ist, durch die Fernsprechauskunft der Fernmeldeämter nicht entgegenstehen, weil es sich dabei um veröffentlichte Daten handelt, die jedermann zur Verfügung stehen.

Nach der bereichsspezifischen Regelung des § 39 Abs. 2 Fernmeldeordnung werden die Fernsprechteilnehmer mit ihrem Namen in die amtlichen Fernsprechbücher nach der Buchstabenfolge eingetragen. Nur dann, wenn der Name allein für das Auffinden der Rufnummer nicht ausreicht, sind die Lage der Sprechstelle oder andere für das Auffinden der Rufnummer notwendige Angaben, z. B. die Berufsbezeichnung, in den Eintrag aufzunehmen.

Zu 6.6. Registrierung der Verbindungsdaten von Telefongesprächen bei belästigenden Anrufen

Der Bundesbeauftragte für den Datenschutz sieht die Deutsche Bundespost verpflichtet, nicht nur das Rechtsschutzbedürfnis des Angerufenen zu unterstützen, gegen Beleidigungen bzw. Belästigungen vorzugehen, sondern auch das des Anrufers, sich gegen etwaige falsche Anschuldigungen zu wehren.

Eine Änderung der derzeitigen Praxis hält die Deutsche Bundespost aus folgenden Gründen nicht für erforderlich:

Die Deutsche Bundespost teilt die Auffassung des Bundesbeauftragten für den Datenschutz nicht, wonach die Inhaber des beobachteten Anschlusses nach Abschluß der Beobachtung über die Aufzeichnung der von seinem Anschluß ausgegangenen Gespräche informiert und ihm der Name des Inhabers des angerufenen Anschlusses genannt werden sollte. Die Deutsche Bundespost kann keinesfalls sicher sein, daß es sich tatsächlich um belästigende Anrufe handelte, da sie vom Inhalt der Gespräche keine Kenntnis nimmt. Zudem erscheint es auch im Hinblick auf das Recht der Mitbenutzer des beobachteten Anschlusses

auf Wahrung des Fernmeldegeheimnisses nicht unbedenklich, dem Inhaber des beobachteten Anschlusses die vom Bundesbeauftragten für den Datenschutz geforderten Mitteilungen zu machen, da die Deutsche Bundespost nicht einfach davon ausgehen kann, daß die Anrufe ausschließlich vom Anschlußinhaber ausgingen.

In den Fällen, in denen die Deutsche Bundespost dem angeblich belästigten Teilnehmer (Antragsteller) keine Verbindungen mit dem Anschluß des Teilnehmers, den der Antragsteller als Belästiger vermutete, bestätigen kann, wäre eine nachträgliche Information überflüssig und könnte zu Reaktionen, z. B. Privatklage gegen den Antragsteller wegen Beleidigung, führen. Dies könnte manchen belästigten Antragsteller abhalten, im Mißbrauchsfall zur Feststellung ankommender Verbindungen die Beobachtung zu beantragen. Auch in Fällen, in denen die Deutsche Bundespost dem Antragsteller bestätigt, daß vom Anschluß des als Belästiger vermuteten Teilnehmers Anrufe ausgegangen sind, kann der Antragsteller ein Interesse daran haben, von dieser Tatsache keinen Gebrauch zu machen. Auch insoweit besteht kein Rechtsschutzbedürfnis des Inhabers des Anschlusses, von dem die Anrufe ausgingen.

Diese Auffassung widerspricht auch nicht den inhaltsgleichen Beschlüssen des Post- und des Innenausschusses zur Aufzeichnung und Bekanntgabe von Einzelgesprächsdaten. Aus ihnen kann keine Verpflichtung der Deutschen Bundespost zur Unterrichtung des betroffenen Anschlußinhabers über die wegen Verdachts belästigender Anrufe auf Antrag erfolgte Schaltung einer Zählervergleichseinrichtung hergeleitet werden.

Zu 6.7. *Weitergabe von Telefonkundenanschriften zu Werbezwecken*

Der Bundesbeauftragte für den Datenschutz empfiehlt, nur dann eine Adressenweitergabe an die Deutsche Postreklame GmbH vorzusehen, wenn der Fernsprechteilnehmer dieser Übermittlung ausdrücklich zugestimmt hat.

Zur Verfahrensweise sowie zur Frage einer Schadensminderung und -begrenzung bei versehentlicher Weitergabe einer gesperrten Anschrift an die Deutsche Postreklame bemerkt der Bundesminister für das Post- und Fernmeldewesen:

Die Deutsche Bundespost hat das Verfahren zur Übermittlung der Anschriften der Fernsprechteilnehmer an die Deutsche Postreklame GmbH geändert, damit Fehler vermieden werden. Die internen Datenschutzbeauftragten wurden beauftragt zu prüfen, ob die Sperren der Anschriften richtig durchgeführt werden.

Ab Anfang 1987 sollen die Sperren automatisch zusammen mit der Datenübergabe aus dem Änderungsdienst monatlich an die Deutsche Postreklame GmbH weitergeleitet werden. Damit wird das Verfahren sicherer und die Bearbeitungszeit verkürzt.

Eine weitere Verkürzung des Zeitraums zwischen den nachträglich vom Teilnehmer gegen die Weitergabe erhobenen Einwendungen und der Sperre der Anschrift ist mit vertretbarem Aufwand nicht zu realisieren.

Eine Schadensminderung oder Schadensbegrenzung ist im Falle einer versehentlichen Weitergabe einer gesperrten Anschrift nicht möglich.

Ein bezifferbarer Schaden dürfte im Falle der versehentlichen Weitergabe einer Anschrift kaum entstehen. Da Einwendungen des Teilnehmers die versehentlich erfolgte Weitergabe der Anschrift nicht rechtswidrig machen, entsteht ein Ersatzanspruch weder nach haftungsrechtlichen Vorschriften der Fernmeldeordnung noch nach dem derzeitig gültigen Datenschutzrecht.

Die Übermittlung der Adressen der Teilnehmer von den Fernmeldeämtern an die Deutsche Postreklame GmbH ist nach Ansicht der Deutschen Bundespost aufgrund des § 11 Satz 1 BDSG und des § 12 Abs. 2 Fernmeldeordnung auch ohne Zustimmung der Teilnehmer zulässig. Der Innenausschuß des Deutschen Bundestages hat bei der Diskussion des Siebenten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz in seiner Sitzung vom 22. Januar 1986 von der vorgesehenen Änderung der Formblätter zustimmend Kenntnis genommen.

Auch der Bundesbeauftragte für den Datenschutz hat das neue Formblatt in datenschutzrechtlicher Sicht als wesentliche Verbesserung bezeichnet.

Zu 6.8. *Ermittlung von Anschriften Neugeborener durch Postzusteller*

Nach Meinung des Bundesbeauftragten für den Datenschutz ist nicht auszuschließen, daß die Aufforderung der Deutschen Bundespost an ihre Zusteller, Anschriften von Neugeborenen mitzuteilen, im Einzelfall einen Anreiz zur Durchbrechung des Post- und des Amtsgeheimnisses darstellt.

Der Bundesminister für das Post- und Fernmeldewesen weist darauf hin, daß die Pflicht des Postzustellers zur Amtsverschwiegenheit weder die Kenntnis von der Geburt eines Kindes noch die Anschrift der Eltern umfaßt. Beide Angaben sind davon nach § 61 Abs. 1 Satz 2 Bundesbeamtengesetz in doppelter Hinsicht ausgenommen, denn sie stellen im Zustellbezirk offenkundige Tatsachen dar und bedürfen — ebenso wie die Existenz eines Menschen — keiner Geheimhaltung.

Im Gegensatz zum Amtsgeheimnis schützt das Postgeheimnis nicht alle postdienstlichen Vorgänge, sondern nur den der Deutschen Bundespost in Postsendungen aufgrund des einzelnen Postbenutzungsverhältnisses anvertrauten individuellen Postverkehr (§ 5 Abs. 1 Nr. 1 und 2 PostG; vgl. § 354 Abs. 2 Nr. 1 und 2 StGB). Außerhalb dieses Anwendungsbereichs bleibt somit die ganze weitere amtliche Tätigkeit des Postzustellers und das, was er dabei erfährt oder bemerkt. Dazu gehören sämtliche Wahrnehmungen nicht nur

bei Gelegenheit des Dienstes, sondern auch — abgesehen vom individuellen Postverkehr — in Ausübung des Dienstes. Dazu zählt vor allem die Anschrift einer Person als offenkundige Tatsache außerhalb eines konkreten Postverkehrs. Die postalische Anschrift gehört nicht zum Inhalt des Postbenutzungsverhältnisses, sondern ist Voraussetzung für dessen Zustandekommen (OVG Koblenz, NJW 1981, Seite 837 = PostRE 2.05.2.5 Nr. 19, S. 41, 42; Altmannsperger: Gesetz über das Postwesen, Kommentar, 1973, Stand 1984, § 5, Rdnr. 40, 61 und 64).

Im übrigen soll der Zusteller die Anschriften Neugeborener nicht etwa — was mit dem Postgeheimnis vereinbar wäre — von Postsendungen ablesen, sondern lediglich aufgrund seines allgemein häufigen Kontakts zu den Bewohnern seines Zustellbezirks mitteilen.

Postanschriften dürfen somit ohne Verstoß gegen Amts- oder Postgeheimnis vom Zusteller dem Postamt mitgeteilt und von diesem zur Werbung für Postsparbücher genutzt werden.

In der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkt 6.6.1) hält der Deutsche Bundestag es für notwendig, daß die unterschiedlichen Auffassungen über die Anwendbarkeit des BDSG bei neuen Techniken mit kurzer, technisch bedingter Vorhaltedauer rechtlich eindeutig geklärt werden.

Die Deutsche Bundespost ist nach wie vor der Ansicht, daß die Speicherung der Daten i. S. von § 2 Abs. 2 Nr. 1 BDSG voraussetzt, daß eine Informationsquelle mit der Möglichkeit des Zugriffs geschaffen wird. Werden dagegen Daten nur kurzzeitig, oft nur für Sekundenbruchteile festgehalten, liegt keine Datenspeicherung vor, da solche Vorgänge nicht dazu dienen, Informationen aufzubewahren. Solche Vorgänge haben regelmäßig ihre Ursachen in der besonderen Art und Weise technischer Abläufe und damit nur systeminterne Bedeutung. Diese Auffassung wird im übrigen nicht nur durch die Begründung zum Entwurf eines BDSG gestützt (Reg.-Entw., BT-Drucks. 7/1027, S. 23, Begründung zu § 3), sondern auch durch § 13 BDSG, der voraussetzt, daß auf gespeicherte Daten zugegriffen werden kann.

Zu 7. Verkehrswesen

Zu 7.1. (7.1.1. bis 7.1.4.) Fahrzeugregistergesetz (ZEVIS)

Die Darlegungen und Vorschläge beziehen sich auf den Gesetzentwurf der Bundesregierung zur Änderung des Straßenverkehrsgesetzes, mit dem u. a. auch für ZEVIS eine besondere bereichsspezifische Rechtsgrundlage geschaffen werden soll. Dieser Gesetzentwurf liegt dem Deutschen Bundestag zur Beschlußfassung vor (Drucksache 10/5343). Er enthält eine umfassende Regelung über die Erhebung, Speicherung und Nutzung der notwendigen Daten.

Zu 9. Statistik

Zu 9.1. Volkszählungsgesetz und Mikrozensusgesetz

Der Bundesbeauftragte für den Datenschutz stellt am Beispiel des Volkszählungsgesetzes und des Mikrozensusgesetzes heraus, daß im Bereich der amtlichen Statistik die Bemühungen des Deutschen Bundestages, der Bundesregierung und der Behörde des Bundesbeauftragten für den Datenschutz um einen überzeugenden Datenschutz erfolgreich waren.

Die Bundesregierung nimmt diese Feststellung mit Befriedigung zur Kenntnis. Die Anregungen, die der Bundesbeauftragte für den Datenschutz während des parlamentarischen Beratungsverfahrens gegeben hat (z. B. Einrichtung eines wissenschaftlichen Beirats zum Mikrozensus), sind vom Bundesminister des Innern aufgegriffen und bereits realisiert worden. Der Beirat wird entsprechend dem Votum des Deutschen Bundestages auch bei der Durchführung der Volkszählung mitwirken.

Zu 9.2. Handels- und Gaststättenzählung

Die Bemerkungen des Bundesbeauftragten für den Datenschutz zur Durchführung der Handels- und Gaststättenzählung enthalten die Aufforderung, die Verwendung von Namen, Anschrift und Gewerbekennziffer künftig gesetzlich zu regeln.

Der Bundesminister des Innern stellt hierzu fest, daß in der Begründung des Gesetzentwurfs vom 10. November 1978 ausdrücklich ein Hinweis auf die Verwendungsmöglichkeit dieser Angaben für Repräsentativerhebungen enthalten ist. Eine allgemeingültige gesetzliche Regelung für Adreßdateien, wie sie der Bundesbeauftragte für den Datenschutz fordert, ist in § 13 des Entwurfs eines Bundesstatistikgesetzes von der Bundesregierung vorgeschlagen.

Der Bundesbeauftragte für den Datenschutz prüft derzeit, ob die Finanzbehörden im Zusammenhang mit der Handels- und Gaststättenzählung durch Übermittlung der Steuernummern der betroffenen Unternehmen an die statistischen Landesämter gegen das Steuergeheimnis oder andere Geheimhaltungsvorschriften verstoßen haben.

Der Bundesminister der Finanzen vertritt in Übereinstimmung mit den obersten Finanzbehörden der Länder die Auffassung, daß durch die Übermittlung der Steuernummern die Pflicht zur Wahrung des Steuergeheimnisses nicht verletzt wird. Mit der Bekanntgabe der Steuernummern wird den statistischen Landesämtern nicht mehr offenbart, als sich bereits aus der nach § 6 Abs. 2 Handelsstatistikgesetz zulässigen Übermittlung der Anschriften und Gewerbekennziffern der betroffenen Unternehmen ergibt. Die Übermittlung der Steuernummern stellt deshalb schon begrifflich keine Offenbarung im Sinne des § 30 AO dar. Im übrigen dient die Übermittlung der Steuernummern der technischen Durchführung des Verfahrens. Sie soll Rückfragen der statistischen Landesämter bei den Finanzämtern erleichtern und Fehlleitungen sol-

cher Rückfragen, die das Steuergeheimnis gefährden, ausschließen.

Zu 9.3. Hochschulstatistikgesetz

Der von der Bundesregierung am 29. Januar 1986 beschlossene Gesetzentwurf trägt den Anforderungen des Bundesbeauftragten für den Datenschutz in vollem Umfang Rechnung.

Zu 9.4. Bundesstatistikgesetz

Der Bundesbeauftragte für den Datenschutz stellt in seinen Anmerkungen zum Volkszählungsgesetz und zum Mikrozensusgesetz die dort gefundenen verfahrenssichernden Regelungen als beispielhaft für statistische Rechtsvorschriften heraus.

Die Bundesregierung stellt hierzu fest, daß auch der von ihr vorgelegte Entwurf eines Bundesstatistikgesetzes diese Regelungen in allgemeiner Form für die übrigen statistischen Rechtsvorschriften übernimmt. Damit ist dem grundsätzlichen Anliegen des Bundesbeauftragten für den Datenschutz in wesentlichen Punkten bereits Rechnung getragen.

Einzelne kritische Anmerkungen sind zum Teil bereits in einer Übergangsregelung des Gesetzentwurfs berücksichtigt, zum Teil sind sie in der Begründung aufgegriffen und erläutert. Ob weitere datenschutzrechtliche Bestimmungen in den Gesetzentwurf aufzunehmen sind, muß den parlamentarischen Beratungen vorbehalten bleiben.

Zu 10. Sozialwesen

Zu 10.1. Bundeserziehungsgeldgesetz

Der Bundesbeauftragte für den Datenschutz bemängelt, daß einige von ihm vorgeschlagene klarstellende bzw. ergänzende Regelungen zum Referentenentwurf eines Bundeserziehungsgeldgesetzes nicht berücksichtigt worden sind.

Der Bundesminister für Jugend, Familie, Frauen und Gesundheit führt hierzu an, daß der Referentenentwurf des Gesetzes dem Bundesbeauftragten für den Datenschutz mit Schreiben vom 13. Februar 1985 zugeleitet worden ist. Daraufhin hat der Bundesbeauftragte für den Datenschutz mit Schreiben vom 26. Februar 1985 einige klarstellende bzw. ergänzende Regelungen vorgeschlagen.

Die Bundesregierung hat diese Anregungen des Bundesbeauftragten für den Datenschutz im Gesetzgebungsverfahren weitgehend berücksichtigt. Zu den beiden vom Bundesbeauftragten für den Datenschutz im Achten Tätigkeitsbericht jetzt noch angeführten Punkten bemerkt der Bundesminister für Jugend, Familie, Frauen und Gesundheit:

Die Verwendung der nach dem Bundeskindergeldgesetz erhobenen Daten für die Berechnung des einkommensabhängigen Erziehungsgeldes ist durch § 12 Abs. 3 Bundeserziehungsgeldgesetz gewährleistet. Für die umgekehrte Regelung besteht nach der Praxis kein Bedürfnis. Soweit es sich um die Zahlung von Kindergeld für das erste Kind handelt, erfolgt diese einkommensunabhängig, so daß eine Übernahme von Daten, die zum Erziehungsgeld erhoben worden sind, ausscheidet. Die Gewährung von Kindergeld für das zweite Kind und weitere Kinder ist einkommensabhängig, und zwar vom ersten Monat an. Der Berechtigte wird also zunächst der Kindergeldbehörde sein Jahreseinkommen darlegen müssen. Da das Erziehungsgeld erst ab dem 7. Monat einkommensabhängig ist, wird der Berechtigte hierfür auf die Angaben zum Kindergeld verweisen können. Der umgekehrte Fall, daß solche Angaben beim Erziehungsgeld bereits vorliegen, wenn der Antrag auf Gewährung von Kindergeld gestellt wird, erscheint dagegen kaum vorstellbar.

Soweit im übrigen die Bundesanstalt für Arbeit sowohl für das Kindergeld als auch für das Erziehungsgeld zuständig ist, werden Kindergeld und Erziehungsgeld für ab dem 1. Januar 1986 geborene Kinder mit einem Antragsvordruck beantragt. Der Berechtigte weiß also, daß die hier erhobenen Daten in beiden Verfahren verwendet werden. Es kann bei dieser Sachlage also nur fraglich sein, ob bei Mehrkindfällen für das Erziehungsgeldverfahren auch die in der Vergangenheit nur für das Kindergeldverfahren erhobenen Daten verwendet werden dürfen. Dies ist durch § 12 Abs. 3 Bundeserziehungsgeldgesetz ausdrücklich geregelt.

Der Wortlaut des § 6 Abs. 1 Satz 1 und 2 Bundeserziehungsgeldgesetz stimmt im wesentlichen mit § 11 Abs. 1 Bundeskindergeldgesetz überein. Nach Meinung der Bundesregierung ist die Notwendigkeit, die einzelnen Einkunftsarten anzugeben, bereits jetzt hinreichend klargestellt. Aus der Tatsache, daß die Summe der positiven Einkünfte maßgebend ist, diese aber im Einkommensteuerbescheid nicht ausgeworfen sind, ergibt sich nach Meinung der Bundesregierung, daß der Antragsteller die einzelnen Summanden darlegen muß. Insoweit wird auf die Stellungnahme der Bundesregierung zum Sechsten Tätigkeitsbericht (11.3) und zum Siebenten Tätigkeitsbericht (13.4) verwiesen.

Zu 10.4. Arbeitsverwaltung

Der Bundesbeauftragte für den Datenschutz bemängelt, daß im Arbeitslosenhilfeverfahren Einkommensnachweise von Unterhaltspflichtigen an das Arbeitsamt bisher über den Arbeitslosen vorgelegt werden müssen.

Nach Mitteilung des Bundesministers für Arbeit und Sozialordnung wird die Bundesanstalt für Arbeit dieses Verfahren ändern. Angehörige des Arbeitslosen können zukünftig die Einkommensnachweise dem Arbeitsamt auch unmittelbar zusenden.

Die Arbeitslosenhilfebescheide können nach Auffassung des Bundesministers für Arbeit und Sozialordnung dagegen nicht in dem vom Bundesbeauftragten für den Datenschutz gewünschten Sinn geändert wer-

den. Nach § 35 des Zehnten Buches Sozialgesetzbuch hat der Direktor des Arbeitsamtes die Entscheidung zu begründen, wenn einem Antrag auf Arbeitslosenhilfe wegen der Berücksichtigung von Unterhaltsansprüchen nicht oder nicht in vollem Umfang entsprochen wird. Ist der Unterhaltsanspruch gerichtlich oder vertraglich nicht festgestellt, so darf sich die Begründung nicht auf die Angabe des „Unterhaltsanrechnungsbetrages" beschränken. Vielmehr sind alle Tatsachen anzugeben, die es dem Arbeitslosen ermöglichen, die Berechnung des Unterhaltsanspruches zu überprüfen. Hierzu gehört auch das Einkommen des Unterhaltspflichtigen. Es ist nicht verständlich, daß der Bundesbeauftragte für den Datenschutz diese Argumentation in diesem Zusammenhang nicht akzeptiert. Er selbst benutzt die gleiche Argumentation nämlich im Zusammenhang mit der Behandlung ärztlicher Unterlagen (5.1.2) und hält sie dort für zwingend, obwohl die vom Arzt offenbarten Angaben in der Regel weit sensibler sind als die Angabe des Einkommens.

Der Bundesbeauftragte für den Datenschutz verlangt Klarstellung in Rundschreiben und Merkblättern, daß das Arbeitsamt Vermittlungsvorschläge an den Arbeitgeber nicht ohne Wissen des Arbeitnehmers machen darf.

Der Bundesminister für Arbeit und Sozialordnung bemerkt hierzu, daß die Bundesanstalt für Arbeit in einer Besprechung der Leiter der Abteilungen Arbeitsvermittlung der Landesarbeitsämter auf die Rechtslage hingewiesen hat. Die Niederschrift hierüber ist an alle Dienststellen gegangen.

Die Bundesanstalt für Arbeit wird in einem Merkblatt für Benutzer der Arbeitsvermittlung und Arbeitsberatung unter einem gesonderten Abschnitt „Datenschutz" u. a. darauf hinweisen, daß Bewerbungsunterlagen nur mit Zustimmung des Betroffenen an Stellenanbieter weitergegeben werden dürfen.

Nach den Vereinbarungen der Bundesanstalt für Arbeit mit den Länderfinanzbehörden übermitteln die Länderfinanzbehörden der Bundesanstalt Daten über das anrechenbare Einkommen eines Kindergeldberechtigten, wenn dieser damit einverstanden ist (vgl. auch § 21 Abs. 4 SGB X).

Der Bundesbeauftragte für den Datenschutz berichtet von Fällen, in denen der Abgleich auch ohne die Einwilligung des Berechtigten stattfand.

Die Fehlerursache ist nach Auffassung des Bundesministers für Arbeit und Sozialordnung darin begründet, daß der Sachbearbeiter angewiesen ist, in die Zahlungsanweisung an die Datenverarbeitung die Steuernummer des Betroffenen dann und nur dann einzutragen, wenn im Kindergeldantragsformular die Einwilligung erklärt ist. Die Eintragung der Steuernummer löst den maschinellen Datenabgleich aus.

In zunächst 13 Arbeitsämtern sind insoweit weisungswidrige Verfahren festgestellt worden. Die Bundesanstalt für Arbeit hat deshalb angeordnet, daß dort alle Fälle zu überprüfen sind, die in den Datenabgleich einbezogen waren. Im übrigen sind stichprobenweise Überprüfungen angeordnet worden. Die zugesagten Überprüfungen sind erfolgt. Da bei einigen weiteren Arbeitsämtern die Stichproben Zweifel an der weisungsgemäßen Verfahrensweise ergeben haben, mußten auch diese Vollprüfungen vornehmen.

Dagegen ist eine Überprüfung aller bereits in den Datenabgleich einbezogenen rund 1 Million Fälle dem Bundesbeauftragten für den Datenschutz aus gutem Grund nie zugesagt worden. Der Bundesbeauftragte für den Datenschutz sieht einen Organisationsmangel darin, daß in die Anweisung an die Datenverarbeitung kein Hinweis darauf eingetragen gewesen sei, ob die Zustimmung vorliegt. Insoweit verkennt er die Funktion der Anweisung. Darin wird nicht mit „ja/nein" angekreuzt, ob Anspruchsvoraussetzungen oder Verfahrenserfordernisse erfüllt sind. Dies hat der Sachbearbeiter vorher zu prüfen. Kindergeld ist nur anzuweisen, wenn alle Anspruchsvoraussetzungen und Verfahrenserfordernisse erfüllt sind. Eine Steuernummer sowie Name und Geburtstag des Ehegatten sind nur einzutragen, wenn die Zustimmung zum Datenabgleich vorliegt. Im Interesse einer guten Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz ist in diesem besonderen Falle die Kindergeld-Verfügung dem Wunsche des Bundesbeauftragten für den Datenschutz entsprechend systemwidrig mit Ankreuzmöglichkeiten versehen worden. Etwaige Fehler können hierdurch aber nicht ausgeschlossen werden; wer fehlerhaft eine Zustimmung zum Datenabgleich annimmt und deshalb die Steuernummer etc. einträgt, wird auch immer „ja" ankreuzen.

Der Bundesbeauftragte für den Datenschutz kritisiert den Dienstblatt-Runderlaß 128/85 über die Durchführung des Sozialdatenschutzes im Bereich des Ärztlichen Dienstes der Bundesanstalt für Arbeit. Die Bundesanstalt hat in diesem Erlaß die für den Ärztlichen Dienst relevanten Datenschutzregelungen der für den Gesamtbereich der Bundesanstalt geltenden Weisungen zusammengefaßt und auf die spezifischen Belange des Ärztlichen Dienstes ausgerichtet. Zugleich sind in diesem Erlaß die für den Ärztlichen Dienst relevanten Datenschutzregelungen im Zusammenhang mit der Durchführung bestimmter Fachaufgaben anderer Abteilungen eingearbeitet. Dies geschieht u. a. durch Verweisung auf die entsprechenden, die Durchführung der Fachaufgaben regelnden Runderlasse. Damit beinhaltet der Runderlaß 128/85 bereits die vom Bundesbeauftragten für den Datenschutz angeregten zusammenfassenden Weisungen für den Bereich des Ärztlichen Dienstes. Eine noch weitergehende Zusammenfassung ist nicht möglich, weil der Ärztliche Dienst keine originären Aufgaben hat, sondern nur zur Durchführung der der Bundesanstalt übertragenen fachlichen Aufgaben der Abteilungen eingeschaltet wird. Adressat der vom Bundesbeauftragten für den Datenschutz angesprochenen verschiedenen Runderlasse ist nicht primär der Ärztliche Dienst. Es sind die Fachabteilungen, für die die Geltung allgemeiner Weisungen für den Ärztlichen Dienst verwirrend wäre.

Die Bundesanstalt für Arbeit wird eine ähnliche zusammenfassende Regelung wie für den Ärztlichen Dienst auch für den Psychologischen Dienst erlassen.

Zu 10.6. Gesundheitswesen

Zu 10.6.1. Ärztliche Entlassungsberichte

Die Auffassung des Bundesbeauftragten für den Datenschutz, daß ärztliche Kurentlassungsberichte nach den Regeln über die ärztliche Schweigepflicht nur mit Einwilligung des Patienten an den behandelnden Hausarzt und nur im Rahmen des Erforderlichen (§ 69 Abs. 1 Nr. 1 SGB X) an Krankenkassen übermittelt werden dürfen, wird von der Bundesregierung geteilt.

Im einzelnen ist noch nicht abschließend geklärt, in welchem Umfang die Übersendung der Kurentlassungsberichte erforderlich ist.

Ein erster sinnvoller Ausgangspunkt ist es, in der Regel nur Blatt 1 des Kurentlassungsberichts den Krankenkassen zu übersenden. Dieses Blatt enthält Angaben zur Identifizierung des Betroffenen, Behandlungsstätte und Behandlungsort, Aufnahme- und Entlassungsdatum, Diagnosen, ärztlich verordnete Schonungszeiten, Angaben zur Krankheitsursache, zur Krankenhausvorbehandlung, zur Arbeitsunfähigkeitszeit, zur Entlassungsform und Vorschläge für weitere Rehabilitationsmaßnahmen.

Es bleibt jedoch zulässig, daß die Krankenkasse im Einzelfall weitere Teile des Kurentlassungsberichts anfordert, wenn sie zu dem Schluß kommt, daß sie zur Entscheidung über weitere Rehabilitationsmaßnahmen benötigt. Die Verbände der Rentenversicherung und der Krankenversicherung wollen durch Aufstellung von Erforderlichkeits-Katalogen versuchen, für die Zukunft genauere Maßstäbe zu erarbeiten.

Zu 11. Öffentliche Sicherheit

Zu 11.1. Kontrollen und Ergebnisse

Zu 11.1.1. Bundeskriminalamt (BKA)

Zu den zusammenfassenden Wertungen des Bundesbeauftragten für den Datenschutz bezüglich der Datenverarbeitung beim BKA wird auf die Stellungnahme zu Nummer 11.4 und Nummer 12 Bezug genommen.

Zu 11.1.2. Bundesgrenzschutz

Bei der Überprüfung der Datenverarbeitung der Fahndungsleitstelle der Grenzschutzdirektion sind im Zusammenhang mit dem im Aufbau befindlichen neuen Grenzaktennachweis (GAN) des Grenzschutzeinzeldienstes vom Bundesbeauftragten für den Datenschutz aus seiner Sicht bedenkliche Maßnahmen der Datenverarbeitung festgestellt worden. Der Bundesminister des Innern nimmt hierzu wie folgt Stellung:

Der Aufbau des GAN erfolgte z. Z. der datenschutzrechtlichen Prüfung in der Grenzschutzdirektion nach dem Entwurf einer Errichtungsanordnung, der mit dem Bundesbeauftragten für den Datenschutz mehrfach diskutiert wurde und über den weitgehend Einigkeit besteht. Es gibt lediglich zu einigen Bestimmungen unterschiedliche Auffassungen, die bis in die jüngste Vergangenheit mit dem Bundesbeauftragten für den Datenschutz weiter erörtert wurden.

Die in dem Bericht wiedergegebenen tatsächlichen Feststellungen bei der Überprüfung der Fahndungsleitstelle der Grenzschutzdirektion betreffen zum Teil Fälle, in denen noch nicht nach den mit dem Bundesbeauftragten für den Datenschutz unstreitigen Bestimmungen des Entwurfs der Errichtungsanordnung verfahren wurde. Hierzu sind inzwischen entsprechende Anweisungen ergangen, die die künftige Beachtung dieser Bestimmungen sicherstellen sollen. Dazu zählt u. a. auch die Weisung an die Grenzschutzdirektion, daß die befaßten Beamten und Angestellten durch Lehrgänge an der Schule des Grenzschutzeinzeldienstes und durch dezentrale Fortbildungsveranstaltungen bei den Grenzschutzämtern zu schulen sind, um eine ordnungsgemäße Handhabung der Datenverarbeitung zu gewährleisten.

Soweit die Kritik sich auf die Fälle bezieht, in denen die Grenzschutzdirektion nach Bestimmungen des Entwurfs verfahren hat, für die nach Auffassung des Bundesbeauftragten für den Datenschutz die Rechtsgrundlage fehlt bzw. die von ihm nicht für erforderlich gehalten werden, hat der Bundesbeauftragte für den Datenschutz seine Auffassung in einer Stellungnahme gegenüber dem Bundesminister des Innern noch einmal konkretisiert. Es handelt sich einmal um die Frage, in welchen Fällen der von anderen Polizeidienststellen zugegangenen Fahndungsinformationen ein „Grenzbezug" zukommt. Danach bemißt sich, ob diese Information im Grenzaktennachweis gespeichert werden muß. In einer Reihe anderer Fälle hält der Bundesbeauftragte für den Datenschutz die im Entwurf der Errichtungsanordnung vorgesehenen Speicherfristen für zu lang.

Nach erneuter Überarbeitung und Abstimmung mit dem Bundesbeauftragten für den Datenschutz wurde die Errichtungsanordnung GAN zwischenzeitlich in Kraft gesetzt.

Die mit der Wahrnehmung grenzpolizeilicher Aufgaben beauftragten Polizeibehörden der Länder wurden um Prüfung gebeten, ob sie die Eingabe- und Zugriffsberechtigung auf den Bestand des GAN für erforderlich halten.

Der Entwurf der Richtlinien für die Führung personenbezogener Grenzakten (Ri GAN) wurden dem Bundesbeauftragten für den Datenschutz inzwischen ebenfalls zur Stellungnahme zugeleitet.

Zu 11.1.3. Bundesamt für Verfassungsschutz (BfV)

Wie bereits im Vorjahr wird vom Bundesbeauftragten für den Datenschutz bestätigt, daß die informationelle Zusammenarbeit des BfV mit ausländischen Diensten aus datenschutzrechtlicher Sicht insgesamt positiv zu bewerten ist. Zu den angeblich in diesem Bereich noch erforderlichen Verbesserungen ist dem Bundesbeauftragten für den Datenschutz am 6. Januar 1986 vom Bundesminister des Innern eine umfangreiche

Stellungnahme übermittelt worden, die u. a. folgende Aussagen enthält:

Die Beanstandung, daß bei dem Informationsaustausch des BfV mit ausländischen Diensten bei Auskünften aus staatsanwaltlichen oder polizeilichen Erkenntnissen vorrangige gesetzliche Zuständigkeiten für die Übermittlung nicht beachtet werden, ist unberechtigt. So regelt z. B. § 74 (nicht § 73) IRG die Zuständigkeit für Entscheidungen über ausländische Rechtshilfeersuchen. Bei Anfragen ausländischer Dienste an das BfV handelt es sich jedoch nicht um Rechtshilfeersuchen. Bei der Übermittlung von Informationen wird vom BfV auf die rein nachrichtendienstliche Zweckbestimmung ausdrücklich hingewiesen.

Die vom Bundesbeauftragten für den Datenschutz in diesem Zusammenhang ebenfalls zitierten § 1 Abs. 2 und § 10 BKAG regeln den Dienstverkehr des BKA im Bereich der Verbrechensbekämpfung. Die Übermittlung von Informationen durch das BfV an ausländische Dienststellen erfolgt jedoch nicht zu diesem Zweck. Im übrigen darf das BfV Erkenntnisse, die ihm zulässigerweise von der Polizei mitgeteilt worden sind, im Rahmen seiner Aufgaben und Befugnisse unter Berücksichtigung schutzwürdiger Belange des Betroffenen an ausländische Dienste weitergeben. Über die Zulässigkeit der Verwendung der Daten für nachrichtendienstliche Zwecke (und somit eine evtl. Zweckänderung) ist bereits bei der Übermittlung von der Polizei an den Verfassungsschutz entschieden worden.

Zu der Auffassung, daß bei Sicherheitsüberprüfungen des BfV für ausländische Dienste BZR-Erkenntnisse nur verwertet werden dürfen, wenn die Voraussetzungen des § 57 BZRG erfüllt sind, ist dem Bundesbeauftragten für den Datenschutz mitgeteilt worden, daß sich die dem BfV nach § 3 Abs. 2 BVerfSchG obliegende Mitwirkungspflicht bei der Sicherheitsüberprüfung von Personen vor dem Hintergrund der von der Bundesrepublik Deutschland eingegangenen völkerrechtlichen Bindungen nicht auf das Inland beschränken kann. So verpflichten z. B. die aufgrund internationaler Verträge (NATO, WEU-Vertrag, Euratom, EUROCONTROL) von den zuständigen Ministerräten beschlossenen Abkommen und Verordnungen die Mitgliedstaaten u. a., personelle Sicherheitsüberprüfungen nach bestimmten Normen für ihre jeweiligen Staatsangehörigen durchzuführen. Als Besonderheit kommt für die Bundesrepublik Deutschland die Verpflichtung nach Artikel 3 des Zusatzabkommens zum NATO-Truppenstatut hinzu, auch bei der Sicherheitsüberprüfung von Beschäftigten der Stationierungsstreitkräfte mitzuwirken. Die Mitwirkung des BfV nach § 3 Abs. 2 BVerfSchG in diesem Bereich ist deshalb als eigene Sicherheitsaufgabe i. S. des § 41 Abs. 1 Nr. 3 BZRG anzusehen. Im übrigen wird vom BfV niemals der reine Inhalt des Registerauszugs an ausländische Dienste weitergegeben. Die BZR-Auskunft ermöglicht vielmehr lediglich die Prüfung von Sachverhalten, die zu einer Verurteilung geführt haben, anhand der Verfahrensakten. Das Ergebnis dieser Prüfung kann — muß aber nicht — in das Sicherheitsvotum des BfV einfließen.

Zu der Forderung des Bundesbeauftragten für den Datenschutz nach Präzisierung des Anfragegrundes, wenn das BfV bei inländischen Behörden um Auskunft zur Beantwortung von Anfragen ausländischer Dienste bittet, nimmt der Bundesminister des Innern wie folgt Stellung:

Durch die Begründung von Ersuchen des BfV an andere Behörden könnte eine Offenlegung der Maßnahmen des BfV eintreten und damit ihr Zweck gefährdet oder der Betroffene mehr als notwendig beeinträchtigt werden. § 9 Abs. 2 des Entwurfs für eine Neufassung des BVerfSchG (Artikel 3 des Gesetzentwurfs, Drucksache 10/4737) sieht deshalb vor, daß Ersuchen des BfV an Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, nicht begründet zu werden brauchen. Wenn das BfV im Rahmen der Anfrage eines befreundeten Dienstes inländische Behörden um Auskunft bittet, braucht es deshalb weder den Verwendungszweck anzugeben noch mitzuteilen, an wen die Auskunft möglicherweise weitergeleitet wird.

Zu 11.1.6. Zusammenfassende Würdigung

Die Bundesregierung begrüßt die Feststellung des Bundesbeauftragten für Datenschutz, alle Sicherheitsbehörden des Bundes hätten sich im Dialog mit ihm bemüht, die datenschutzrechtlichen Aspekte verstärkt zu berücksichtigen. Dabei unterstreicht der Bundesbeauftragte für den Datenschutz auch als besonders erfreulich den stetigen Abbau älterer Speicherungen beim BKA.

Andererseits hat der Bundesbeauftragte für den Datenschutz Vorbehalte gegen den Ausbau der Datenverarbeitung beim BKA und kommt zu dem Schluß, die „technische Entwicklung habe sich schrittweise vom geltenden Recht entfernt". Dieser Aussage widerspricht die Bundesregierung. Es ist irreführend, rechtspolitische Forderungen und Idealvorstellungen mit dem geltenden Recht gleichzusetzen. Nach dem Volkszählungsurteil sind auch für den Bereich der polizeilichen Informationsverarbeitung bereichsspezifische Rechtsvorschriften zu erlassen. Es ist jedoch nach ständiger Verfassungsgerichtsrechtsprechung anerkannt, daß im Rahmen eines Übergangsbonus das alte Recht anwendbar bleibt (vgl. speziell zur polizeilichen Informationsverarbeitung BayVerfGH, Entscheidung vom 9. Juli 1985, DVBl. 1986, Seite 35).

Wie vom Bundesbeauftragten für den Datenschutz angeregt, bietet es sich an, im Zuge der Vorbereitung von gesetzgeberischen Maßnahmen auf dem Gebiet der polizeilichen Informationsverarbeitung in der 11. Legislaturperiode die Praxis der Datenverarbeitung darzustellen. Dem entspricht auch die Zielrichtung der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkte 8.2 und 8.4.2). Dieser Bitte kann jedoch nur außerhalb dieser Stellungnahme in einem gesonderten Bericht gegenüber dem Innenausschuß des Deutschen Bundestages entsprochen werden.

Die Bundesregierung geht davon aus, daß es im Zuge der beabsichtigten Novellierung des Polizeirechts, insbesondere auch des BKA-Gesetzes und des BGS-Gesetzes, gelingen wird, zu Lösungen zu kommen, die einen sachgerechten Ausgleich zwischen den datenschutzrechtlichen Belangen und den Notwendigkeiten polizeilicher Aufgabenerfüllung darstellen. Die Bundesregierung erwartet, daß damit auch grundsätzliche Probleme geklärt werden, die der Bundesbeauftragte für den Datenschutz in seinem Tätigkeitsbericht wiederum aufgezeigt hat. Es ist beabsichtigt, den Bundesbeauftragten für den Datenschutz auch weiterhin bereits bei der Erarbeitung der bereichsspezifischen Entwürfe zu beteiligen.

Zu 11.2. Gesetzgebungsvorhaben und deren datenschutzrechtliche Bewertung

Zu den unter Berücksichtigung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz erarbeiteten Gesetzentwürfen zur Neuregelung des Polizei- und Verfassungsschutzrechts vertritt der Bundesbeauftragte für den Datenschutz die Auffassung, daß die Entwürfe dem Gebot der Normenklarheit noch nicht hinreichend Geltung verschafften und im Ergebnis darauf hinausliefen, die gegenwärtige Praxis festzuschreiben und zum Teil sogar erheblich zu erweitern.

Hinsichtlich der Ergänzung des Musterentwurfs eines einheitlichen Polizeigesetzes weist der Bundesminister des Innern darauf hin, daß sich die kritischen Bemerkungen des Bundesbeauftragten für den Datenschutz auf eine überholte Entwurfsfassung beziehen. Aufgrund weiterer Beratungen in den Gremien der IMK ist der Entwurf zwischenzeitlich, insbesondere unter datenschutzrechtlichen Gesichtspunkten, erheblich präzisiert worden. Der Bundesbeauftragte für den Datenschutz hat Gelegenheit erhalten, zu der überarbeiteten Fassung Stellung zu nehmen. Der Musterentwurf stellt weitgehend auf die Aufgabenstellung der Polizeibehörden der Länder ab. Deshalb kann eine gleichförmige Übernahme des Musterentwurfs für den Bund wegen der spezifischen Aufgabenstellung von BKA und BGS nicht in Betracht kommen. Vielmehr ist beabsichtigt, in der 11. Legislaturperiode das BKA-Gesetz und das BGS-Gesetz sowie die StPO zu novellieren.

Zu den übrigen im Tätigkeitsbericht angesprochenen Gesetzesvorhaben (VerfSchG, ZAG, MAD-G) wird vom Bundesminister des Innern folgendes bemerkt:

Die von der Bundesregierung durch Kabinettsbeschluß vom 29. Januar 1986 verabschiedeten Gesetzentwürfe zur Änderung des Bundesverfassungsschutzgesetzes sowie zur Schaffung eines MAD-Gesetzes und eines Gesetzes über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden des Bundes und der Länder in Angelegenheiten des Staats- und Verfassungsschutzes (Zusammenarbeitsgesetz) ziehen erstmals durchgreifende Konsequenzen aus dem Volkszählungsgesetzurteil des Bundesverfassungsgerichts für den Datenschutz und die Sicherheitsbehörden. Der Bund hat damit gegenüber den Ländern die Vorreiterrolle bei der Umsetzung des Volkszählungsurteils übernommen und ein Beispiel für eine umfassende Verwirklichung der Grundsätze des Volkszählungsgesetzurteils gegeben. Dies wird u. a. bei der Regelung über die Befugnisse der Verfassungsschutzbehörden deutlich. Die alte Generalklausel in § 3 BVerfSchG wurde durch 11 nach Art, Umfang und Inhalt der Datenerhebung und -verarbeitung differenzierende, detaillierte Regelungen ersetzt.

Die Entwürfe schreiben nicht allein die derzeitige Praxis der Informationserhebung und -verarbeitung bei den Sicherheitsbehörden fest, sondern ihre Zulässigkeit und ihr Umfang wurden gemäß den vom Bundesverfassungsgericht im Volkszählungsgesetzurteil festgelegten Maßstäben kritisch überprüft und in dem vom Bundesverfassungsgericht geforderten Umfang durch ins einzelne gehende Aufgaben- und Befugnisnormen konkretisiert und begrenzt. Die Gesetzentwürfe enthalten für die Sicherheitsbehörden z. B. folgende Beschränkungen:

— Verbot des Datenverbundes:

  Ein automatisierter Datenverbund zwischen Polizei und Nachrichtendiensten wird nicht mehr zugelassen. Gleiches gilt für die Nachrichtendienste untereinander. Ausnahmen sind nur für die Verfassungsschutzbehörden in den Tätigkeitsfeldern Spionageabwehr und Terrorismusbekämpfung sowie für Aktensuchdateien und bei Vorliegen einer Genehmigung der zuständigen Innenminister möglich.

— Verbot der Datensammlung auf Vorrat:

  Die Anlage von Aktensammlungen und Dateien ist nur noch in den genau beschriebenen Aufgabenbereichen der Nachrichtendienste zulässig. Die Entwürfe präzisieren, daß die Nachrichtendienste nicht sammeln dürfen, was ihnen nützlich erscheint, sondern sie sind strikt an den sogenannten Erforderlichkeitsgrundsatz gebunden.

— Verbot von Geheimdateien:

  Die Errichtung von automatisierten Dateien ist — ähnlich wie nach den Dateienrichtlinien für das Bundeskriminalamt — nur noch mit vorheriger Zustimmung des politisch verantwortlichen Ministers zulässig. Er muß genehmigen, welche Daten über wen gesammelt werden dürfen und wer hiervon Kenntnis erlangen soll.

— Verbot unkontrollierter Datenströme:

  Der Informationsaustausch zwischen den Sicherheitsbehörden wird eingegrenzt; in Präzisierung des datenschutzrechtlichen Erforderlichkeitsgrundsatzes wird eine strenge Bindung an diesen Grundsatz normiert.

— Verbot der Übermittlung von personenbezogenen Informationen durch mit Staats- und Verfassungsschutzaufgaben betraute Behörden an andere Stellen außerhalb des Bereichs des Staats- und Verfassungsschutzes, sofern die Übermittlung nicht ausdrücklich durch den Gesetzgeber zugelassen ist. Diese Regelung trägt dem Zweckbindungsprinzip Rechnung und entspricht der Vorgabe des Bun-

desverfassungsgerichts, wonach Zweckdurchbrechungen nur aufgrund förmlicher gesetzlicher Grundlagen zugelassen werden dürfen.

— Gebot zum Nachbericht:

Wenn sich Informationsübermittlungen der Nachrichtendienste als unvollständig oder unrichtig erweisen, sind diese gesetzlich verpflichtet, dies zu berichtigen.

— Verfahrensrechtliche Schutzvorschriften:

Z. B. Schutzbestimmungen für Minderjährige, Pflicht zur Führung eines Verzeichnisses bzw. zur Aktenkundigmachung für Ersuchen der Nachrichtendienste, spezielle Unterrichtungspflicht gegenüber der Parlamentarischen Kontrollkommission im Zusammenarbeitsgesetz.

Der Bundesbeauftragte für den Datenschutz beanstandet, daß im Bereich der Zollverwaltung seine Kontrollkompetenz bestritten und Kontrollen dadurch verhindert würden.

Im Rahmen des Steuerbereinigungsgesetzes 1986 sind die rechtlichen Grundlagen für das Zollkriminalinstitut (ZKI) und die allgemein materiellen Voraussetzungen für Art und Umfang der Datenverarbeitung des ZKI geschaffen worden. Der Bundesminister der Finanzen bereitet den Entwurf für die nach § 12 Abs. 5 Finanzverwaltungsgesetz vorgesehene Rechtsverordnung unter Beteiligung des Bundesbeauftragten für den Datenschutz vor.

Zwischen dem Bundesbeauftragten für den Datenschutz und dem Bundesminister der Finanzen bestehen gegensätzliche Rechtsauffassungen über die Einengung der Kontrollbefugnis durch das Steuergeheimnis nach § 30 AO. Der Bundesbeauftragte für den Datenschutz wurde wiederholt vom Bundesminister der Finanzen darauf hingewiesen, daß die Regelung des Steuergeheimnisses keine für seine Kontrollkompetenz erforderliche Ausnahmeregelung zugunsten der Datenschutzkontrolle enthält.

Die unterschiedlichen Auffassungen sind z. Z. nicht überbrückbar.

Eine Bereinigung der Meinungsverschiedenheiten wird im Rahmen der Novellierung des BDSG angestrebt.

Im Hinblick auf die Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkt 8.6), wonach der Deutsche Bundestag eine gesetzliche Regelung des Verhältnisses von Datenschutzprüfung und Steuergeheimnis auch für den Bereich der Steuer- und Zollfahndung für dringend geboten ansieht, bezieht sich der Bundesminister der Finanzen auf seine vorstehende Stellungnahme. Im übrigen wird auf die Stellungnahme zu 11.5. verwiesen.

Zu 11.3. Datenschutz bei der Sicherheitsüberprüfung

Die gemäß Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkt 8.3) erbetene Prüfung, ob und inwieweit unter Berücksichtigung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz eine gesetzliche Regelung der Sicherheitsüberprüfung erforderlich ist, wird vom Bundesminister des Innern bereits durchgeführt.

Bei Datenerhebungen und -speicherungen im Rahmen von Sicherheitsüberprüfungen fordert der Bundesbeauftragte für den Datenschutz neben einem Höchstmaß an Transparenz für die Betroffenen auch ein grundsätzliches Verwertungsverbot für andere Zwecke. Ausnahmen von diesem Verwertungsverbot dürfen nach seiner Auffassung nur für die Spionageabwehr und für mit § 7 Abs. 3 G 10 vergleichbare Fallgruppen zulässig sein.

Für den Bereich des BfV ist zu dieser Forderung zu bemerken, daß der Verfassungsschutz als Einheit anzusehen ist. Die Beobachtung rechts- und linksextremistischer Bestrebungen steht als gleichrangige Aufgabe neben der Abwehr terroristischer und geheimdienstlicher Aktivitäten. Im übrigen zeigt der Werdegang von Terroristen, daß sie häufig zunächst durch extremistische Betätigung aufgefallen sind. Wenn also z. B. durch eine Sicherheitsüberprüfung bekannt wird, daß der zu Überprüfende einer (u. U. militanten) extremistischen Organisation angehört, kann dies auch der für die Beobachtung dieser extremistischen Bestrebung zuständigen Abteilung des BfV mitgeteilt werden, unabhängig davon, ob die Voraussetzungen des § 7 Abs. 3 G 10 vorliegen.

Ob über die beabsichtigte Neufassung des BVerfSchG (insbesondere mit seinen §§ 5 und 6 Abs. 1 und 3) hinaus eine gesetzliche Regelung der Sicherheitsüberprüfung erforderlich bzw. sinnvoll ist, wird von der Bundesregierung noch geprüft.

Zu 11.4. Internationale Zusammenarbeit der Sicherheitsbehörden und internationaler Datenschutz bei den Sicherheitsbehörden

Zu 11.4.1. Verstärkung der internationalen Zusammenarbeit

Der Bundesbeauftragte für den Datenschutz weist darauf hin, daß wegen der allgemeinen Internationalisierung der Kriminalität und des Abbaus von Grenzkontrollen die Notwendigkeit der verbesserten internationalen Zusammenarbeit der Sicherheitsbehörden, insbesondere auch beim personenbezogenen Informationsaustausch, besteht. Der Bundesbeauftragte für den Datenschutz geht zu Recht davon aus, daß die an sich wünschenswerte Angleichung des Datenschutzrechts in Verbindung mit den Befugnissen zur Informationsverarbeitung in den einzelnen Staaten nicht oder zumindest kurzfristig nicht zu erreichen sein wird.

In Abstimmung mit dem Bundesbeauftragten für den Datenschutz hat die Bundesregierung den EG-Partnern im Rahmen der Verhandlungen über Ausgleichsmaßnahmen beim Abbau der Grenzkontrollen die Vereinbarung folgender datenschutzrechtlicher Mindeststandards vorgeschlagen:

— Der übermittelnde Staat trifft Vorsorge, daß die übermittelten Daten richtig, erforderlich und verhältnismäßig in bezug auf die vom Empfänger beabsichtigte Nutzung sind. Über wesentliche Änderungen ist nachzuberichten.

— Die Nutzung der Daten durch den Empfänger wird auf polizeiliche oder sonstige gesetzlich festgelegte Zwecke beschränkt. Auf die nach nationalen Bestimmungen geltenden Löschungsfristen ist hinzuweisen. Nach Ablauf der jeweils für die übermittelnde Stelle geltenden Löschungsfristen ist eine weitere Verwertung grundsätzlich nicht mehr zulässig.

— Die polizeilichen personenbezogenen Daten sind grundsätzlich nach Wegfall der Erforderlichkeit zu löschen. Es sind regelmäßige Überprüfungen der Erforderlichkeit der Daten vorzusehen. Außerdem sind Bestimmungen über die Dauer der Aufbewahrung und die Berichtigung der Daten zu treffen.

— Es sind interne Überwachungs- und Kontrollverfahren für die Verarbeitung von personenbezogenen Daten durch die Polizei entsprechend den jeweils bestehenden Regelungen über die Zusammenarbeit mit dem Datenschutzbeauftragten zu erlassen.

— Die Sicherheit der übermittelten Daten ist zu gewährleisten. Unberechtigter Zugang oder unerlaubte Übermittlung sind zu verhindern.

Zu 11.4.2. Verstärkung des internationalen Datenschutzes

Die Bundesregierung unterstützt das Anliegen der Datenschutzbeauftragten, auf die Dauer zu einheitlichen Regelungen über den internationalen Informationsaustausch im Polizeibereich zu kommen. Dabei ist darauf hinzuweisen, daß unterhalb der Gesetzesschwelle bereits in erheblichem Umfang detaillierte Regelungen bestehen. Zu nennen sind vor allem die innerstaatlichen KpS- und Dateienrichtlinien sowie das Interpol-Datenstatut. Die Erarbeitung ergänzender Richtlinien zum Interpol-Datenstatut betreffend die Löschungsvorschriften beim Generalsekretariat von Interpol und den Informationsaustausch zwischen den Nationalen Zentralbüros, mit der die Interpol-Gremien befaßt sind, ist noch nicht abgeschlossen.

Der Bereich des internationalen Informationsaustausches im Polizeibereich wird in Konsequenz aus dem Volkszählungsurteil des Bundesverfassungsgerichts auch Gegenstand der bereichsspezifischen Gesetzgebung sein. Es ist aber aus der Sicht der Bundesregierung nicht unproblematisch, für diesen Bereich zu weitgehende Forderungen für differenziertere gesetzliche Regelungen oder internationale Vereinbarungen zu erheben, die — gerade auch im internationalen Vergleich — nicht erfüllt werden können. Unter diesem Gesichtspunkt bedarf der vom Bundesbeauftragten für den Datenschutz angesprochene Entwurf einer Konvention des Europarates noch näherer Prüfung.

Zu 11.5. Kontrollbefugnis des Bundesbeauftragten für den Datenschutz der Steuer- und Zollfahndung

Der Bundesbeauftragte für den Datenschutz beanstandet, daß ihm bei Prüfungen im Bereich der Zollfahndung die Einsicht in Unterlagen unter Berufung auf das Steuergeheimnis versagt werde.

Der Bundesminister der Finanzen stellt fest, daß das Steuergeheimnis lediglich die Einsichtnahme in Unterlagen bestimmter Personen verbietet, es sei denn, die Einwilligung des Betroffenen liegt vor oder die Unterlagen lassen keine Rückschlüsse auf bestimmte Personen zu. Insoweit stehen sie auch im Bereich der Zollfahndung für Prüfungen durch den Bundesbeauftragten für den Datenschutz zur Verfügung.

Zwischen der Zollverwaltung und den Polizeien des Bundes und der Länder ist für eine wirksame Bekämpfung der Rauschgiftkriminalität (Rauschgiftschmuggel und -handel) seit Anfang der 70er Jahre ein Meldedienst eingerichtet (Polizeidienstvorschrift 386.1). Von der Zollverwaltung im Rahmen des Meldedienstes (Nachrichtenaustausch) übermittelte Informationen, bei denen es sich neben Falldaten auch um personenbezogene Daten handelt, werden von den Polizeidienststellen in der Falldatei Rauschgift beim Bundeskriminalamt gespeichert. Das Steuergeheimnis steht der Offenbarung der Rauschgiftdaten nicht entgegen (§ 30 Abs. 4 Nr. 4 a oder Nr. 5 a AO).

Die Rechtsausführungen des Bundesbeauftragten für den Datenschutz stehen nicht im Einklang mit § 30 AO. Der Bundesbeauftragte für den Datenschutz verkennt, daß für den von ihm in seinem Bericht angesprochenen Meldedienst eine gesetzliche Bestimmung vorhanden ist, die die Durchbrechung des Steuergeheimnisses für diesen Zweck ausdrücklich zuläßt, während eine entsprechende ausdrückliche Bestimmung für die Einsichtnahme des Bundesbeauftragten für den Datenschutz in steuerliche Unterlagen fehlt. Insoweit geht auch sein Hinweis auf § 19 BDSG fehl. Nicht jede Regelung, die eine umfassende Auskunftsverpflichtung der Behörden statuiert, vermag auch die Regelungen über die Wahrung des Steuergeheimnisses zu durchbrechen. Erforderlich ist vielmehr eine gesetzliche Regelung, die die Offenbarung steuerlicher Verhältnisse ausdrücklich zuläßt. Der Wortlaut des § 30 Abs. 4 Nr. 2 AO ist insoweit eindeutig.

Zu 12. Bundeskriminalamt (BKA)

Zu 12.1. Probleme aus der Datenverarbeitungsstruktur beim BKA

Die Argumentation des Bundesbeauftragten für den Datenschutz bezüglich der zunehmenden Dateienvielfalt erscheint widersprüchlich. Folgt man der

These, es sei eine zunehmende Dateienvielfalt festzustellen und dies sei datenschutzrechtlich bedenklich, so wäre die notwendige Konsequenz die Einrichtung einer übergreifenden Datei mit allen Informationen für alle Polizeivollzugsdienststellen mit der Möglichkeit des Direktabrufs von jeder Stelle auf alle Daten. Gerade datenschutzrechtliche Forderungen haben jedoch bei der Fortschreibung des INPOL-Konzeptes 1981 dazu geführt, keinen zentralen Personenindex (ZPI) für alle INPOL-Anwendungen zu schaffen. Die INPOL-Konzeption geht davon aus, daß unterschiedliche und selbständige Dateien wie z. B. Personenfahndungsdatei, Kriminalaktennachweis, Haftdatei etc. geführt werden, die allerdings den nur einmal geführten Personendatensatz nutzen.

Die Bundesregierung hat bereits in der Stellungnahme zum Siebenten Tätigkeitsbericht darauf hingewiesen, daß gerade auch die Anforderungen des Datenschutzes dazu führen, Informationen in verschiedenen Dateien zu verarbeiten. Auf diese Weise ist es möglich, die jeweils relevanten Informationen unter Beachtung des Erforderlichkeitsgrundsatzes zu steuern (z. B. Zugriffsbeschränkungen innerhalb des INPOL-Systems bezüglich bestimmter Dienststellen und bestimmter Datenbestände) bzw. sonst differenziert zu verarbeiten.

Es trifft nicht zu, es sei „nur aus der Struktur der Datenverarbeitung heraus erklärlich", daß eine ganze Reihe von Errichtungsanordnungen personengebundene Hinweise im P-Datensatz vorsehen. Vielmehr wird der notwendige Informationsumfang für jede Datei gesondert geprüft und in Errichtungsanordnungen festgelegt. So sind z. B. in der Datei „Personenfahndung" die vom Bundesbeauftragten für den Datenschutz genannten (Nummer 12.3) verschiedenen personengebundenen Hinweise möglich, während etwa in der Datei „Kriminalaktennachweise" nur ein Teil von ihnen vorgesehen ist. Die Tatsache, daß in der besonders angesprochenen Falldatei „Rauschgift" alle vorgesehenen personengebundenen Hinweise ausgegeben werden können, hängt damit zusammen, daß es sich nicht um eine bloße Hinweisdatei handelt wie beim Kriminalaktennachweis; vielmehr werden in diesem herausragenden Kriminalitätsbereich alle relevanten Fallinformationen zusammengeführt. Dazu gehören auch die personengebundenen Hinweise.

Der Bundesbeauftragte für den Datenschutz verbindet die Darstellung, die INPOL-Konzeption ermögliche dateiübergreifende Recherchen, mit der Ansicht, daß dabei über den jeweils konkreten Zweck der einzelnen Datei hinausgegangen würde. Dazu ist darauf hinzuweisen, daß es selbstverständliche Aufgabe kriminalpolizeilicher Auswertungsarbeit ist, bei Bedarf auch die Querbezüge zwischen den Informationen in den einzelnen Dateien herzustellen. Es wäre z. B. unvertretbar, die Auswertung einer Rauschgiftdatei nur zu Zwecken der Rauschgiftbekämpfung zulassen zu wollen, da sich Bezüge zu anderen Kriminalitätsbereichen ergeben können (z. B. Vermögensdelikte als „Rauschgiftbeschaffungstaten", organisierte Kriminalität u. a.). Andererseits können für die Fallbearbeitung eines Rauschgiftdelikts zusätzlich relevante Informationen neben der Falldatei Rauschgift auch in anderen INPOL-Anwendungen (z. B. PIOS-Rauschgiftdatei, Haftdatei, Datei Erkennungsdienst usw.) gespeichert sein. Es ist daher grundsätzlich von einem einheitlichen Zweck der polizeilichen Datenverarbeitung auszugehen. Bei der übergreifenden Recherchemöglichkeit geht es also nicht, wie der Bundesbeauftragte für den Datenschutz anklingen läßt, „um die Angleichung des Datenverarbeitungsrechts an die vorgesehene technische Struktur". Vielmehr folgt die technische Struktur den Notwendigkeiten kriminalpolizeilicher Auswertungsarbeit.

Zur Klarstellung ist in diesem Zusammenhang jedoch erneut zu betonen, daß die Errichtungsanordnungen für Dateien des BKA bezüglich der Daten „anderer Personen" jeweils strenge Zweckbindungsregelungen vorsehen (vgl. Stellungnahmen der Bundesregierung zum Siebenten Tätigkeitsbericht Nummer 19.2.1, zum Sechsten Tätigkeitsbericht Nummer 17.4.2 und Nummer 18.3.3 und zum Fünften Tätigkeitsbericht Nummer 3.2.1). In diesen Fällen ist insoweit eine dateiübergreifende Recherche ausgeschlossen.

Der Bundesbeauftragte für den Datenschutz spricht — unabhängig von einem erledigten Einzelfall — die Frage an, ob „es hinnehmbar ist, daß sich das BKA auf den Standpunkt stellt, die Löschungsfrist in einer Datei sei nicht zu beachten, wenn die betreffende Person auch noch in einer anderen Datei mit einer längeren Frist erfaßt ist". Hier schließt der Bundesbeauftragte für den Datenschutz in unzulässiger Weise von einer Einzelfrage auf einen generellen Sachverhalt, der so nicht zutrifft. Es ist hervorzuheben, daß sich — entgegen dem vom Bundesbeauftragten für den Datenschutz erweckten Eindruck — die Löschungsfristen nach den Bestimmungen der Errichtungsanordnung für die jeweilige Datei richten und eine isolierte Löschung grundsätzlich dann — nach Einzelfallprüfung — erfolgt, wenn die Speicherung für diese bestimmte Datei nicht mehr erforderlich ist. Allerdings werden die beim BKA anfallenden Informationen auch konventionell in der Kriminalakte des Betroffenen erfaßt. Solange die Kriminalakte aufbewahrt wird, weil in ihr über den Fall hinaus, der zur Speicherung in der bestimmten Datei geführt hat, weitere kriminalpolizeilich relevante Erkenntnisse enthalten sind, muß die Kriminalakte weiterhin auch im Aktennachweissystem erfaßt sein.

Der Bundesbeauftragte für den Datenschutz behauptet, alle Polizeidienststellen, die auf INPOL-Bund Zugriff hätten, würden „bei Benutzung des entsprechenden Operationscodes in jedem Fall die Information erhalten, ob über die angefragte Person Daten in einer anderen Datei gespeichert sind". Dies trifft so nicht zu. Zum einen können die PIOS- und SPUDOK-Anwendungen nicht mit der vom Bundesbeauftragten für den Datenschutz angesprochenen bereichsübergreifenden Anfrage erreicht werden. Diese bezieht sich lediglich auf die Fahndung, den KAN, die Haftdatei, die ED-Datei sowie auf Hinweise auf Bestand in Falldateien. Zum anderen haben die Grenzdienststellen vor Ort lediglich Zugriff auf die INPOL-Personen- und Sachfahndung sowie den (eigenen) Grenzaktennachweis, nicht dagegen auf den KAN, die Haftdatei etc. Ihnen steht demzufolge auch die bereichsübergrei-

fende Anfrage nicht zur Verfügung. Für sachbearbeitende Kriminaldienststellen jedoch ist die bereichsübergreifende Anfrage an die genannten Standarddateien erforderlich. Diese Dienststellen haben sämtlich Zugriff auf diese Einzeldateien. Vielfach ist es aus kriminaltaktischer Sicht erforderlich, alle diese Einzeldateien abzufragen, weil es auch um eine ganzheitliche, nicht lediglich deliktsbezogene Betrachtung eines Straftäters geht. Es wäre für den Sachbearbeiter schlechterdings nicht einsehbar, wenn er mehrere Einzelanfragen starten müßte. Ein datenschutzrechtlicher Gewinn wäre darin nicht zu sehen. Im übrigen muß nochmals hervorgehoben werden, daß es grundsätzlich nicht angeht, innerhalb des einheitlichen Zwecks der Kriminalitätsbekämpfung weiter zu differenzieren.

Zu 12.2. Kriminalaktennachweis — Theorie und Praxis

Der Bundesbeauftragte für den Datenschutz vertritt erneut die Auffassung, das Konzept über den Kriminalaktennachweis (KAN) mit der Beschränkung auf schwere Fälle oder solche mit überregionaler Bedeutung für die zentrale Speicherung überlagere die anderen INPOL-Anwendungen; soweit andere INPOL-Verfahren, wie z. B. die erkennungsdienstliche Datei, diese Differenzierung nicht nachvollziehen, würde das KAN-Konzept unterlaufen.

Die Bundesregierung hat wiederholt ihre Auffassung zu diesen Fragen dargelegt. Insbesondere in der Stellungnahme zum Fünften Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz hat die Bundesregierung anläßlich der Frage des Verhältnisses des KAN zur zentralen ED-Datei beim BKA ausführlich und in grundsätzlicher Weise Stellung genommen (vgl. Drucksache 10/1719 — Anhang, zu Nummer 3.3.6). Der Grundannahme des Bundesbeauftragten für den Datenschutz, das BKA dürfe in allen Bereichen/Dateien nur Fälle von schwerer und überregional bedeutsamer Kriminalität speichern, kann nicht gefolgt werden. Die seinerzeitigen Ausführungen gelten auch für die vom Bundesbeauftragten für den Datenschutz jetzt angesprochene Falldatei Rauschgift und den BKA-Aktennachweis (BKA-AN).

Zu 12.3. Personengebundene Hinweise und Gefahr der sozialen Abstempelung

Der Bundesbeauftragte für den Datenschutz hält — auch unter Hinweis auf einen Beschluß der Datenschutzbeauftragten des Bundes und der Länder — die Verwendung der personengebundenen Hinweise (PHW) in Polizeidateien für datenschutzrechtlich problematisch und regt eine Beschränkung auf die Fahndungsdatei sowie eine Reduzierung des Katalogs der PHW an.

Das Bundeskriminalamt hält die Verwendung der PHW weiterhin für erforderlich. Sie dienen vorwiegend dem Zweck der Eigensicherung der Beamten, vermitteln aber auch Hinweise auf taktisch richtiges Verhalten dem Betroffenen gegenüber und wirken sonst auch ermittlungsfördernd.

Die Gremien der IMK werden sich in Kürze mit der Frage der Verwendung der PHW nochmals befassen.

Zu 12.4. Das fortdauernde Problem der Speicherung „anderer Personen"

Die vom Bundesbeauftragten für den Datenschutz konstatierte stärkere Tendenz, auch sog. „andere Personen" zu erfassen, kann von der Bundesregierung nicht bestätigt werden. Von einer „ständigen Zunahme von PIOS- und SPUDOK-Anwendungen" (das sind Dateien, bei denen die Speicherung von „anderen Personen" in Frage kommt) kann nicht gesprochen werden. Die durchschnittliche Betriebsdauer einer SPUDOK-Datei beläuft sich auf 6 bis 9 Monate. Zudem wird SPUDOK nur in bedeutsamen Fällen eingesetzt.

Hervorzuheben ist, daß es neben den Fristenregelungen gemäß Nummer 4.5 Dateienrichtlinien in den einzelnen Errichtungsanordnungen für Dateien, in denen überhaupt „andere Personen" gespeichert werden dürfen, als weitere Schutzvorkehrung strenge Zweckbindungsregelungen für die Daten „anderer Personen" gibt.

Zur Frage der Rechtsgrundlagen ist die Bundesregierung der Auffassung, daß im Rahmen des bereits erwähnten Übergangsbonus (vgl. oben Nummer 11.1.6) bis zum Erlaß spezieller gesetzlicher Ermächtigungen die Speicherung auf die §§ 161, 163 StPO in Verbindung mit § 2 BKA-G gestützt werden kann.

Zu 12.5. Ungelöste Probleme bei der Abteilung Staatsschutz

Der Bundesbeauftragte für den Datenschutz geht davon aus, daß das BKA gerade im Staatsschutzbereich die Verpflichtung habe, vor Auskunftserteilung aktiv den Verfahrensausgang zu erfahren, wenn dieser nicht bekannt ist.

Die Bundesregierung hat zu den erneut dargelegten Anregungen bereits im Zusammenhang mit dem Sechsten Tätigkeitsbericht Stellung genommen. Sie hat zum Ausdruck gebracht, daß das BKA gerade auch im Staatsschutzbereich bemüht ist, den Zielvorstellungen des Bundesbeauftragten für den Datenschutz entgegenzukommen. Auf die Stellungnahme zum Sechsten Tätigkeitsbericht wird Bezug genommen (vgl. Nummer 18.3.2 i. V. m. Nummer 17.2.2).

Ergänzend ist darauf hinzuweisen, daß das BKA in den vom Bundesbeauftragten für den Datenschutz angesprochenen Fällen (Straftaten von geringerer Bedeutung) dem Verhältnismäßigkeitsgrundsatz regelmäßig durch auf drei Jahre verkürzte Speicherungsfristen Rechnung trägt.

Zu 13. Nachrichtendienste

Nach der Beschlußempfehlung des Innenausschusses des Deutschen Bundestages vom 22. Januar 1986 zum Sechsten und Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Punkt 8.5) ist die datenschutzrechtliche Kontrolle für Maßnahmen nach dem G 10 in Anbetracht der aufgetretenen Unklarheiten alsbald gesetzlich zu regeln.

Die Bundesregierung ist der Auffassung, daß das G 10 als lex spezialis die Kontrolle des Bundesbeauftragten für den Datenschutz im Bereich des G 10 ausschließt (auf die Stellungnahme der Bundesregierung zum Siebenten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz — 21.2.4 — wird hingewiesen).

Es ist vorgesehen, die datenschutzrechtliche Kontrolle für Maßnahmen nach dem G 10 deshalb auch im BDSG klarzustellen. Entsprechend sieht der Gesetzentwurf der Bundesregierung zur Änderung des BDSG in § 19 Abs. 5 Nr. 2 eine Regelung vor, nach der personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 G 10 unterliegen, nur dann vom Bundesbeauftragten für den Datenschutz kontrolliert werden, wenn die Kommission nach Artikel 10 GG den Bundesbeauftragten hierum ersucht.

Zu 13.1. Bundesamt für Verfassungsschutz (BfV)

Zu 13.1.1. Konsequenzen aus der datenschutzrechtlichen Kontrolle bei der Abteilung III

Die vom BfV aufgrund der Prüfung des Bundesbeauftragten für den Datenschutz bei der Abteilung III veranlaßten Maßnahmen werden vom Bundesbeauftragten ausdrücklich begrüßt.

Zu den vom Bundesbeauftragten für den Datenschutz als noch nicht ausreichend bezeichneten Regelungen für die Übermittlung löschungsreifer Daten ist zu bemerken, daß die vom BfV vor der Auskunftserteilung durchzuführende Relevanzprüfung unter Berücksichtigung des Anfragegrundes und des Erkenntnisstandes der anfragenden Behörden nach Auffassung der Bundesregierung datenschutzrechtlichen Anforderungen ausreichend Rechnung trägt.

Hinsichtlich der Führung von Hintergrundmaterial über demokratische Organisationen zur Beurteilung extremistischer Beeinflussungsversuche ist in der Stellungnahme der Bundesregierung zum Siebenten Tätigkeitsbericht (Nummer 21.1.1) bereits darauf hingewiesen worden, daß dieses Material wegen des fehlenden Dateibezuges nicht der Kontrollkompetenz des Bundesbeauftragten für den Datenschutz unterliegt. Im übrigen wird Hintergrundmaterial im BfV ohnehin nur gesammelt, um extremistische Einflüsse auf demokratische Organisationen zutreffend bewerten zu können.

Die Ausführungen des Bundesbeauftragten für den Datenschutz, daß die 15jährige Regelspeicherfrist nicht generell für alle Abteilungen des BfV gelten solle, da zumindest im Extremismusbereich eine kürzere Speicherfrist von max. 10 Jahren angemessen sein dürfte, beziehen sich auf die „NADIS-Löschungsrichtlinien". Diese Richtlinien schreiben vor, daß NADIS-Speicherungen, wenn keine neuen Erkenntnisse anfallen, spätestens nach 15 Jahren auf ihre Relevanz überprüft werden müssen. Diese Überprüfungsfrist verliert jedoch immer mehr an Bedeutung, da die Erforderlichkeit der Speicherung für die Aufgabenerfüllung des BfV im Rahmen der laufenden Facharbeit ständig überprüft wird, eine große Zahl von Erstspeicherungen als Zeitspeicherungen vorgenommen werden (Wiedervorlage zur Relevanzprüfung nach 2 oder 5 Jahren) und darüber hinaus im Rahmen systematischer Überprüfungsaktionen Aktenbestände auch vor Ablauf von 15 Jahren überprüft werden. Von einer 15jährigen „Regelspeicherfrist" im BfV kann daher nicht die Rede sein. Dennoch soll die Frage einer möglichen Verkürzung der Überprüfungsfristen nach den NADIS-Löschungsrichtlinien unter Beteiligung der Länder geprüft werden, da die Richtlinien vom Bundesamt und den Landesbehörden für Verfassungsschutz gemeinsam beschlossen worden sind.

Die Ausführungen des Bundesbeauftragten für den Datenschutz über den Entwurf einer Neufassung des Verkartungsplans der Abteilung III des BfV gehen auf einen Bericht des Bundesministers des Innern zurück, der dem Innenausschuß des Deutschen Bundestages am 22. November 1985 zugeleitet worden ist. Im Februar 1986 sind die im Tätigkeitsbericht genannten Bedenken gegen den Entwurf mit dem Bundesbeauftragten für den Datenschutz erörtert worden, und es wurden Kompromißlösungen vereinbart, die datenschutzrechtlichen Anforderungen entsprechen, ohne die Aufgabenerfüllung der Verfassungsschutzbehörden substantiell zu beeinträchtigen. Insbesondere sind entsprechend der Forderung des Bundesbeauftragten für den Datenschutz, im Verkartungsplan zwischen linksextremistischen Kern- und Nebenorganisationen einerseits und beeinflußten Organisationen andererseits zu differenzieren, Sonderregelungen für Funktionäre, Mitglieder und Anhänger beeinflußter Organisationen vorgesehen. Außerdem wurden mehrere Begriffe präzisiert. Über die mit dem Bundesbeauftragten für den Datenschutz erzielten Kompromisse wird der Innenausschuß des Deutschen Bundestages vom Bundesminister des Innern unterrichtet.

Auch über die vom Bundesbeauftragten für den Datenschutz erwähnten besonderen Dateien des BfV, die u. a. zur Identifizierung von Personen dienen sollen, haben im Februar 1986 Gespräche mit dem Bundesbeauftragten für den Datenschutz stattgefunden. Unterschiedliche Auffassungen bestanden vor allem hinsichtlich des Umfanges der in den Dateien gespeicherten Merkmale. Nachdem der Katalog der Merkmale für den Bereich der Abteilung III des BfV erheblich reduziert worden ist und insbesondere Merkmale, die der Privatsphäre zuzurechnen sind, gestrichen werden, hat der Bundesbeauftragte für den Datenschutz erklärt, daß er die weitere Nutzung der Dateien in ihrer jetzigen Form für vertretbar hält. Über die mit dem Bundesbeauftragten für den Datenschutz abgestimmte Ausgestaltung der besonderen Dateien des BfV, deren Führung zur sachgerechten Beobachtung linksextremistischer Bestrebungen weiterhin erforderlich ist, wird der Innenausschuß des Deutschen Bundestages ebenfalls unterrichtet. Ein Persönlich-

keitsbild im Sinne eines „Totalabbildes", dessen automatisierte Erstellung das Bundesverfassungsgericht für absolut unzulässig erklärt hat (vgl. BVerfGE 65, 53), konnte jedoch auch in der Vergangenheit anhand der besonderen Dateien des BfV nicht erstellt werden, weil eine Reihe wichtiger Lebensbereiche in diesen Dateien nicht erfaßt werden kann.

Zu 13.1.2. Die Weiterentwicklung der Datenverarbeitung beim BfV

Der Bundesbeauftragte für den Datenschutz fordert, daß bei Löschung von Personendaten in NADIS-PZD nach Möglichkeit auch die zugehörigen Akten oder Aktenteile vernichtet werden sollen, da der Zugriff auf solche Akten nach der Löschung zwar schwieriger, ein gezieltes Wiederauffinden von Informationen jedoch anhand anderer Dateien des BfV durchaus möglich sei. Hierzu bemerkt der Bundesminister des Innern:

Werden die Daten einer Person in NADIS-PZD gelöscht, wird auch die zugehörige Personenakte unverzüglich vernichtet bzw. aufgelöst. Darüber hinaus hat das BfV verfahrensmäßig sichergestellt, daß zu der Person ggf. bestehende Speicherungen in anderen Dateien des BfV ebenfalls gelöscht werden. Nach der Löschung personenbezogener Daten, die aus Sachakten des BfV stammen, ist — auch wenn die Akte nicht vernichtet wird — ein gezielter Zugriff auf die Informationen anhand automatisierter Verfahren nicht möglich. Die einzige — rein theoretische — Möglichkeit zum Wiederauffinden von Informationen über Personen, deren Daten bereits gelöscht sind, wäre die Durchsicht der gesamten Sachakten, was schon im Hinblick auf den hohen Arbeitsaufwand nahezu oder gänzlich unmöglich ist. Um auch die theoretische Möglichkeit auszuschließen, daß in Sachakten enthaltene Informationen über Personen nach Löschung der Daten noch verwertet werden, soll vom BfV geprüft werden, in welcher Form in Sachakten auf die Tatsache der Löschung hingewiesen werden kann.

Zu 13.1.3. Sonderdatei im Rahmen der Sicherheitsüberprüfung

Der Bundesbeauftragte hat gegen die Erforderlichkeit und Zulässigkeit einiger Datenfelder der im BfV für Sicherheitsüberprüfungen eingerichteten Sonderdatei Bedenken geäußert.

In welchem Umfang die erwähnte Sonderdatei zur Erfüllung der Mitwirkungsaufgaben des BfV bei der Durchführung von Sicherheitsüberprüfungen erforderlich ist, wird vom Bundesminister des Innern noch geprüft. Vor Erlaß einer Errichtungsanordnung wird dem Bundesbeauftragten für den Datenschutz Gelegenheit zur Stellungnahme gegeben.

Zu 13.2. Militärischer Abschirmdienst

Zu den die Datenverarbeitung im Militärischen Abschirmdienst (MAD) betreffenden Ausführungen des Bundesbeauftragten für den Datenschutz nimmt der Bundesminister der Verteidigung wie folgt Stellung:

Es wird begrüßt, daß der Bundesbeauftragte für den Datenschutz seine bisherigen Bedenken gegen die Verwertung der im Rahmen von Sicherheitsüberprüfungen gewonnenen personenbezogenen Informationen für Zwecke der Spionageabwehr sowie für die Verfolgung von Straftaten in Analogie zu § 7 Abs. 3 G 10 zurückgestellt hat. Der Auffassung des Bundesbeauftragten für den Datenschutz, daß der MAD die bei Sicherheitsüberprüfungen gewonnenen Erkenntnisse nicht für seine übrige Aufgabenerfüllung nutzen oder an andere Behörden übermitteln dürfe, kann aber nicht gefolgt werden.

Zweck der Sicherheitsüberprüfungen ist es festzustellen, ob der Beschäftigung des Betroffenen in einem sicherheitsempfindlichen Bereich Sicherheitsbedenken entgegenstehen. Bei der Prüfung der damit zusammenhängenden Fragen kann auf die Mitwirkung aller Arbeitsbereiche des MAD und ggf. der Verfassungsschutzbehörden des Bundes und der Länder nicht verzichtet werden. Dazu ist eine Weitergabe der personenbezogenen Daten des Betroffenen an diese Stellen unerläßlich. Die vom Bundesbeauftragten für den Datenschutz vorgeschlagene Handhabung hätte zur Folge, daß der Arbeitsbereich des MAD, der mit der Abwehr verfassungsfeindlicher Bestrebungen beauftragt ist, und jede andere Verfassungsschutzbehörde ihre Ermittlungen unabhängig von den Arbeitsbereichen des MAD, denen die Sicherheitsüberprüfung und die Spionageabwehr übertragen ist, durchführen müßten. Dies würde nicht nur einen höheren Verwaltungsaufwand zur Folge haben, sondern auch für die betroffene Person wesentlich belastender sein.

Der vom Bundesbeauftragten für den Datenschutz kritisierten Verfahrensweise steht die dem Betroffenen gegebene Zusicherung, wonach seine Angaben „streng vertraulich" behandelt werden, nicht entgegen. Durch diese Zusicherung wird keine besondere Geheimhaltungspflicht des MAD begründet, sondern lediglich zum Ausdruck gebracht, daß die Angaben des Betroffenen einem besonderen Schutz vor dem Zugang Unbefugter unterliegen und die Verschwiegenheit insofern besonders streng gewahrt wird. Daraus folgt aber nicht, daß der MAD die aus Anlaß der Sicherheitsüberprüfung gewonnenen Daten nicht für alle Arbeitsbereiche nutzen oder in Erfüllung der gesetzlichen Amtshilfepflicht an andere Behörden übermitteln darf.

DER BUNDESMINISTER DES INNERN

Bonn, den 28. Oktober 1987

Stellungnahme der Bundesregierung zu dem Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (BfD)

Zu 1. Gesamtüberblick

Der Beschluß des Deutschen Bundestages vom 10. Dezember 1986 zum Sechsten und Siebenten Tätigkeitsbericht enthält u. a. die Bitte an den Bundesbeauftragten für den Datenschutz, in künftigen Tätigkeitsberichten in der systematischen Darstellung stärker zwischen Rechtsverstößen einerseits und Anregungen andererseits zu unterscheiden.

Der Neunte Tätigkeitsbericht ist nicht so gegliedert worden. Dadurch wird nicht sichtbar, daß bei rund 30 durchgeführten Kontrollen in Behörden und Dienststellen des Bundes nur wenig zu beanstanden war. „Spektakuläres hat sich dabei nicht ergeben, Skandale habe ich nicht aufgedeckt" (Presseerklärung des BfD vom 10. Februar 1987).

Soweit der Tätigkeitsbericht kritische Ausführungen zu verabschiedeten Gesetzen enthält, wird auf eine Stellungnahme dazu verzichtet. Der Bundesbeauftragte ist in den jeweiligen Ausschüssen des Deutschen Bundestages zu allen Gesetzesvorlagen ausführlich angehört worden. Deshalb erscheint eine nochmalige Auseinandersetzung mit den Bedenken des Bundesbeauftragten weder sinnvoll noch geboten. Notwendig ist jedoch der Hinweis darauf, daß die Bundesregierung die zu verabschiedeten Gesetzen geäußerte Rechtsauffassung des Bundesbeauftragten für den Datenschutz (vgl. 10.1 seines Berichts) nicht teilt.

Zu 3. Innere Verwaltung

Zu 3.3. *Personenstandswesen*

Der Bundesbeauftragte für den Datenschutz weist auf die unterschiedlichen Auffassungen des Bundesministers der Finanzen und des Bundesministers des Innern zur sog. „Totenliste" hin. Während nach den Vorstellungen des Bundesministers der Finanzen der Standesbeamte gesetzlich verpflichtet werden sollte, „Sterbefälle nach dem hierfür maßgebenden Muster des Erbschaftsteuer- und Schenkungsteuergesetzes oder der Durchführungsverordnung zu diesem Gesetz in der jeweils geltenden Fassung mitzuteilen", hält der Bundesminister des Innern die von einer Bund-Länder-Arbeitsgruppe vorgeschlagene Verpflichtung des Standesbeamten für ausreichend, dem für die Verwaltung der Erbschaftsteuer zuständigen Finanzamt die im abgelaufenen Monat beurkundeten Sterbefälle mitzuteilen.

Der Bundesminister des Innern wird die Problematik im Rahmen der weiteren Arbeiten an dem Entwurf eines Fünften Gesetzes zur Änderung des Personenstandsgesetzes mit dem Bundesminister der Finanzen weiter erörtern und nach einvernehmlichen Lösungsmöglichkeiten suchen.

Zu 3.4. *Wahlrecht*

Der Bundesbeauftragte für den Datenschutz begrüßt die Feststellung in der Stellungnahme der Bundesregierung zum Achten Tätigkeitsbericht (zu 2.4), daß Behörden nicht verpflichtet sind, Bedienstete zum Zwecke der Bestellung als Wahlhelfer zu benennen. Der Bundesbeauftragte für den Datenschutz regt gleichwohl an, den Behörden und ihren Bediensteten für künftige Wahlen eine geeignete Orientierungshilfe auf der Basis der geltenden Rechtslage an die Hand zu geben.

Der Bundesminister des Innern hat diese Anregung aufgegriffen und die Länder gebeten, ihre Behörden rechtzeitig vor einer Bundestagswahl über die Rechtslage dahin gehend zu unterrichten, daß bei einem Herantreten an Beschäftigungsbehörden zum Zwecke der Benennung von Wahlhelfern auf die Freiwilligkeit hinzuweisen ist.

Zu 4. Rechtswesen

Zu 4.1. *Mitteilungen in Zivilsachen (MiZi)* *Mitteilungen in Strafsachen (MiStra)*

Die vom Bundesbeauftragten für den Datenschutz angekündigte Stellungnahme zu dem Diskussionsentwurf eines „Justizmitteilungsgesetzes" liegt inzwischen dem Bundesminister der Justiz vor.

Der Bundesminister der Justiz wird die Auffassung des Bundesbeauftragten für den Datenschutz bei der Ausarbeitung des Referentenentwurfs ebenso in die weiteren Überlegungen einbeziehen wie die Stellungnahmen der übrigen beteiligten Stellen; diese Stellungnahmen stehen allerdings zum großen Teil noch aus.

Zu 4.2. *Strafprozeßordnung*

Der Bundesbeauftragte für den Datenschutz stellt fest, daß das Strafverfahrensrecht in wesentlichen Bereichen noch keine den Anforderungen der Rechtsprechung des Bundesverfassungsgerichts genügende Vorschriften über den Umgang mit personenbezogenen Daten enthält.

Auch die Bundesregierung sieht insoweit einen Regelungsbedarf, der sich außer den vom Bundesbeauftragten für den Datenschutz angesprochenen Bereichen auch auf den Einsatz verdeckter Ermittler und

eine allgemeine Regelung über die Speicherung und Übermittlung personenbezogener Daten im Rahmen der Strafverfolgung bezieht. Einzelheiten des vom Bundesminister der Justiz erarbeiteten „Arbeitsentwurfs", zu dem auch eine detaillierte Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 24./25. November 1986 vorliegt, bedürfen noch gründlicher Überarbeitung.

Zu 7. Personalwesen

Zu 7.1. Konventionelle Personaldatenverarbeitung

Zu 7.1.2. Beihilfe

— Der Bundesbeauftragte für den Datenschutz begrüßt die beabsichtigte umfassende Neuregelung des Personalaktenrechts. Wie schon in früheren Tätigkeitsberichten weist der Bundesbeauftragte für den Datenschutz erneut auf die Notwendigkeit einer Abschottung der Beihilfestelle von der Personalverwaltung hin.

Die Bundesregierung hat zur Neuregelung des Personalaktenrechts eine interministerielle Arbeitsgruppe beim Bundesministerium des Innern eingesetzt, die sich u. a. auch mit der Problematik der Abtrennung der Beihilfestellen von der allgemeinen Personalverwaltung befaßt. Der Bundesbeauftragte für den Datenschutz ist an der Arbeitsgruppe beteiligt.

— Der Bundesbeauftragte für den Datenschutz hält im übrigen als besonderes Problem das seit Oktober 1985 praktizierte Antragsverfahren für die Beihilfefähigkeit psychotherapeutischer Maßnahmen für bedenklich, da in dem „Bericht an den Gutachter" (Anlage 2 zu Hinweis Nummer 5.2 zu § 6 Abs. 1 Nr. 2 BhV) unter vollständiger Namensnennung Aussagen über Psychogenese und Psychodynamik der neurotischen Entwicklung und über die Prognose der Therapie gefordert werden. Nach Auffassung des Bundesbeauftragten für den Datenschutz sind für die Begutachtung durch den externen Gutachter weder der Name noch das Geburtsdatum des Patienten erforderlich, statt dessen hält der Bundesbeauftragte für den Datenschutz es für ausreichend, wenn in diesem Falle eine Chiffre-Nummer sowie das Alter des Patienten angegeben würde.

Das Anliegen des Bundesbeauftragten für den Datenschutz ist in der Bund-Länder-Kommission für das Beihilferecht erörtert worden.

Die Kommission hat durch eine Änderung des Hinweises Nummer 5.2 zu § 6 Abs. 1 Nr. 1 BhV weitere Schutzmaßnahmen vor versehentlichem Öffnen sowohl des Arztberichts als auch der Stellungnahme des Gutachters durch nicht mit der Beihilfebearbeitung beauftragte Personen vorgesehen.

Zur Chiffrierung des Namens und des Geburtsdatums hat die Kommission dagegen weder zwingende rechtliche noch sachliche Gründe erkennen können, die es rechtfertigen, Kennziffern im Verkehr zwischen zwei gesetzlich und berufsrechtlich der ärztlichen Schweigepflicht unterliegenden Personen einzuführen. Sie ist der Auffassung, daß diese bereits lange vor dem Datenschutz bestehende und bewährte Schweigepflicht weder Anlaß zu Mißtrauen oder Befürchtungen einer möglichen Verletzung noch für zusätzliche, erschwerende bürokratische Auflagen im Verkehr zwischen Ärzten bietet.

— Der Bundesbeauftragte für den Datenschutz äußert die Besorgnis, daß die Beihilfeberechtigten, die zugleich freiwilliges Mitglied der Postbeamtenkrankenkasse sind, nicht hinreichend deutlich darüber informiert sind, daß sie die Rechnungsbelege dem Beihilfe- und Erstattungsantrag im verschlossenen Umschlag beifügen können.

Der Bundesminister für das Post- und Fernmeldewesen weist darauf hin, daß Mitglieder der Postbeamtenkrankenkasse allgemein darüber informiert sind, daß die Rechnungsbelege dem Beihilfe- und Erstattungsantrag auch im verschlossenen Umschlag beigefügt werden können. Es ist bekannt, daß ein Teil der Mitglieder bewußt von dieser Möglichkeit keinen Gebrauch macht. Inzwischen ist hierfür ein Umschlag mit besonderem Aufdruck als Lagerformblatt eingeführt worden. Die Beihilfeberechtigten wurden erneut auf die beiden Möglichkeiten für die Vorlage der Belege hingewiesen.

Zu 7.1.3. Besoldung/Versorgung

— Der Bundesbeauftragte für den Datenschutz stellt fest, daß im Bundesministerium des Innern und seinem Geschäftsbereich Kindergeldakten nicht separat geführt werden, vielmehr werden die anfallenden Unterlagen dem Kostenteil der Personalakte zugeordnet. Der Bundesbeauftragte für den Datenschutz vertritt die Auffassung, daß Kindergeldakten getrennt von den übrigen Personalvorgängen geführt werden müssen.

Der Bundesminister des Innern führt hierzu an, daß gemäß seinem Erlaß betreffend Anlage und Führung der Personalakten vom 21. Juni 1966 an die Dienststellen im Geschäftsbereich die Personalakten in fünf Teile (Teile A bis E) zu gliedern sind. Teil D enthält Zahlungsunterlagen aller Art. Da eine getrennte Führung der Kindergeldakten nicht vorgesehen ist, sind diese zum Teil D zu nehmen.

Durch das gemeinsame Rundschreiben des Bundesministers des Innern und des Bundesministers für Jugend, Familie und Gesundheit vom 26. Oktober 1983 ist sichergestellt, daß Kindergeld-Daten an die mit der Bearbeitung von Personalsachen Betrauten nicht weitergegeben bzw. bei der Bearbeitung von Personalsachen nicht verwendet werden dürfen, sofern Kindergeld- und Personalangelegenheiten von derselben Stelle/Person bearbeitet werden. Eine zusätzliche Trennung der Aktenführung wird zum gegenwärtigen Zeitpunkt unter

dem Gesichtspunkt der Verhältnismäßigkeit des Aufwandes für nicht erforderlich gehalten.

Die Frage der Behandlung von Kindergeldakten ist im übrigen Gegenstand der Beratungen in der interministeriellen Arbeitsgruppe zur Neuordnung des Personalaktenrechts. Vom abschließenden Ergebnis dieser Beratungen wird es abhängen, ob und welche organisatorischen Konsequenzen hinsichtlich der Führung der Kindergeldakten zu ziehen sind. Derzeit sind Maßnahmen daher nicht angebracht, zumal auch bei der heutigen Praxis ein Mißbrauch der Kindergelddaten vom Bundesbeauftragten für den Datenschutz nicht festgestellt worden ist.

— Der Bundesbeauftragte für den Datenschutz hält das derzeitige Verfahren, Steuerbescheide zu den Kindergeldunterlagen zu nehmen, wenn ein Anspruch über den Sockelbetrag hinaus geltend gemacht wird, für änderungsbedürftig.

Nach Auffassung des Bundesministers der Finanzen muß für die Ermittlung der einkommensabhängigen Minderung des Kindergeldes daran festgehalten werden, daß der bei den Akten verbleibende Einkommensteuerbescheid oder die Ablichtung hiervon alle Einkünfte (Einkunftsarten) bis zur Summe der Einkünfte, die Vorsorgeaufwendungen, die Unterhaltsleistungen nach § 10 Abs. 1 Nr. 1 oder § 33 a Abs. 1 EStG sowie die festgesetzten Steuerbeträge erkennen lassen muß. Da der Bundesrechnungshof darauf besteht, daß die Nachprüfung der Entscheidungen über das einkommensabhängige Kindergeld anhand der bei den Akten befindlichen Einkommensnachweise gewährleistet sein muß, kann die Entscheidung darüber, welche Einkunftsarten unkenntlich gemacht werden und welche erkennbar bleiben, nicht dem Berechtigten überlassen werden. Die steuerlich maßgebende Summe der Einkünfte kann neben positiven auch negative Einkünfte umfassen. Die Minderung des Kindergeldes stellt aber allein auf die positiven Einkünfte ab und verbietet den Ausgleich mit Verlusten aus anderen Einkunftsarten (§ 11 Abs. 2 Bundeskindergeldgesetz).

— Der Bundesbeauftragte für den Datenschutz hält das Verfahren, den förmlichen Kassenanweisungen bei Zahlung von Unfallfürsorge Arztrechnungen, Rezepte und sonstige Belege beizufügen, unter Aspekten des Personaldatenschutzes für bedenklich.

Der Bundesrechnungshof vertritt hierzu die Auffassung, im Falle der Unfallfürsorge auf die Beifügung der zahlungsbegründenden Unterlagen im Hinblick auf die §§ 48 und 55 RRO nicht verzichten zu können.

Der Bundesrechnungshof führt dabei aus, daß nach der Rechtsprechung durch Güter- und Interessenabwägung zu ermitteln ist, ob die Pflicht zur Vorprüfung der Unfallfürsorge oder das Recht des Betroffenen an der Geheimhaltung seiner Gesundheitsdaten überwiegt. Nach seiner Auffassung überwiegt der Persönlichkeitsschutz nicht.

Der Bundesrechnungshof vertritt im übrigen die Auffassung, daß — abgesehen von den rechtlichen Erwägungen — bekanntgewordene Betrugsfälle gezeigt haben, daß die Rechnungsbelege einschließlich der zahlungsbegründenden Unterlagen weder bei der anordnenden/sachbearbeitenden Dienststelle noch bei der Bundeskasse verbleiben dürfen. Nicht zuletzt um die Gefahr auch nachträglicher Manipulationen an den Belegen gering zu halten, wird das Beleggut nach der kassenmäßigen Erledigung den Vorprüfungsstellen überantwortet; es gelangt aus dem Bereich der Verwaltung in den Verfügungsbereich der Finanzkontrolle.

Auch im Falle der Beihilfe verbleiben die zahlungsbegründenden Unterlagen nicht bei der Verwaltung. Sie werden hier — ausnahmsweise — den Beihilfeempfängern zurückgegeben, die sie für weitere Erstattungen von dritter Seite benötigen. Solche Erstattungen Dritter gibt es bei den Fällen der Unfallfürsorge nicht.

Schließlich läßt sich die zeitlich vorgezogene Vorprüfung der Beihilfeausgaben vor der Zahlung aus rechtlichen und organisatorischen Gründen nicht auf die Ausgaben der Unfallfürsorge übertragen. Andernfalls würde in weiten Bereichen (vergleichbare Bereiche sind Leistungen wegen Gesundheitsschäden in der Kriegsopferversorgung und Leistungen nach dem Bundesentschädigungsgesetz) eine visaartige Vorprüfung eingeführt, die die Vorprüfungsordnung für die Bundesverwaltung grundsätzlich abgeschafft hat und nur in Ausnahmefällen zuläßt (vgl. Nummer 1.6 VPOB).

Zu 7.1.4. Einzelfälle

Im Rahmen der Wohnungsfürsorge forderte die Bezirksregierung Braunschweig vom Grenzschutzamt Braunschweig, daß einem Belegungsvorschlag für eine Wohnung eine Stellungnahme zu den wirtschaftlichen Verhältnissen des Bewerbers beizufügen sei.

Der Bundesgerichtshof hat in seinem Urteil vom 10. März 1983 — III Z R 169/81 — festgestellt, daß dem Bund bei der Ausübung des Wohnungsbesetzungsrechts die Nebenpflicht erwächst, keinem Bediensteten eine Wohnung zu überlassen, der den Mietzins voraussichtlich nicht tragen kann. Dabei hat er auf die Kenntnis der zuständigen Personaldienststelle abgestellt.

Im übrigen hat sich auf die Ausschreibung hin kein Bediensteter des GS-Amtes Braunschweig beworben.

Eine Stellungnahme über wirtschaftliche Verhältnisse von Bediensteten des GS-Amtes Braunschweig ist daher nicht abgegeben worden.

Zu 7.2. Automatisierte Personaldatenverarbeitung

Zu 7.2.1. Personalinformationssysteme

— Der Bundesbeauftragte für den Datenschutz hat im Deutschen Patentamt das dort betriebene Personalinformationssystem kontrolliert.

Nach den Feststellungen des Bundesbeauftragten für den Datenschutz erscheint der Inhalt der Datenbank des Deutschen Patentamtes „weitgehend problemlos". Soweit der Bundesbeauftragte für den Datenschutz Anregungen gegeben und Änderungsvorschläge gemacht hat, hat der Bundesminister der Justiz mit Schreiben vom 6. November 1986 und 26. März 1987 dazu Stellung genommen.

Trotz der Vorbehalte des Bundesbeauftragten für den Datenschutz hält der Bundesminister der Justiz die Speicherung der Beurteilungsnote — wie auch die Bundesregierung in ihrer Antwort auf die Große Anfrage der Fraktion der SPD zum Personalinformationssystem (Drucksache 10/4594) ausführt — weiterhin für notwendig. Die Speicherung ist angesichts der Personalstärke des Deutschen Patentamts notwendig, um einen ersten Überblick bei der Vorbereitung von Personalentscheidungen zu gewinnen, und dient zur Kontrolle, ob alle vergleichbar beurteilten Mitarbeiter in die Vorauswahl einbezogen wurden.

Der Bundesminister der Justiz bemerkt im übrigen, daß der Umfang der Druckaufträge bereits eingeschränkt wurde. Die Festlegung der Abfragen und des gesamten weiteren Verfahrens erfolgte unter Beteiligung des internen Datenschutzbeauftragten und der Personalvertretung, so daß die Einhaltung des § 15 Nr. 2 BDSG gewährleistet wird.

Die Aufgaben des internen Datenschutzbeauftragten wurde einem weiteren Mitarbeiter übertragen, der dieser Tätigkeit erheblich mehr Zeit widmen kann.

— Der Bundesbeauftragte für den Datenschutz vertritt die Auffassung, daß die Bearbeitung von Beurteilungsnoten in dem vom Bundesminister für Finanzen geplanten Personalbetreuungs- und Informationssystem über das vertretbare Maß hinausgeht.

Der Bundesminister der Finanzen führt hierzu aus: Das nach § 41 Abs. 2 BLV zu bildende Gesamturteil der Beurteilung faßt die Einzelergebnisse der Beurteilung zusammen und bildet nach Rechtsprechung und Kommentierung eine zuverlässige Erkenntnisquelle im Leistungsvergleich der einzelnen Beamten untereinander. Es ermöglicht den Vergleich, auf den bei der sachgerechten Auslese zur Vorbereitung personalrechtlicher Maßnahmen, u. a. der Beförderung, abzuheben ist (vgl. Kommentierung Schröder/Lehmhöfer/Krafft „Das Laufbahnrecht der Bundesbeamten", Randziffer 9 zu § 41 BLV). Entsprechend hatte die Bundesregierung bereits in ihrer Antwort auf die Große Anfrage der Fraktion der SPD zum Personalinformationssystem ausgeführt, daß in der Bundesverwaltung in der Regel nur die Gesamturteile gespeichert werden und auf dieses Merkmal zur Feststellung der Qualifikation und Beförderungseignung vielfach nicht verzichtet werden kann (Drucksache 10/4594 — Antwort zur Frage 2.3 Abschnitt II).

Das Beamten- und Laufbahnrecht kennt im übrigen keine konkrete Festschreibung von einzelnen Beförderungsvoraussetzungen, sondern läßt ausgehend von § 23 i. V. m. § 8 Abs. 1 Satz 2 BBG dem Dienstherrn bewußt einen weiten Gestaltungsspielraum, der von der Rechtsprechung bisher durchgehend bestätigt worden ist. Wesentlich ist, daß die von den einzelnen Dienstherren in diesem Rahmen aufgestellten Beförderungsgrundsätze sachgerecht sind. Es bleibt daher dem pflichtgemäßen Ermessen des einzelnen Dienstherrn überlassen, im Interesse einer einheitlichen und praktikablen Handhabung der Auswahl der zu befördernden Beamten pauschalierende objektive Kriterien für die Bewertung der nach § 23 i. V. m. § 8 BBG maßgebenden Eigenschaften zu bestimmen, sofern diese sachgerecht sind, sich im Rahmen der Gesetze halten und allgemeingültigen Wertmaßstäben nicht widersprechen. In der Rechtsprechung sind dabei Beförderungssysteme, die bei sonst gleicher Eignung, Befähigung und fachlicher Leistung auf das Ergebnis der letzten Beurteilung(en) und das Allgemeine Dienstalter der Beamten abstellen, ausdrücklich als sachgerecht und im zulässigen Ermessensspielraum liegend anerkannt worden.

Der Bundesbeauftragte für den Datenschutz geht offenbar auch von falschen Voraussetzungen hinsichtlich des Zustandekommens der Beurteilungen aus. Die von ihm für die Beförderungsentscheidung angestrebte Informationsbasis wird weitgehend im Rahmen des Beurteilungsverfahrens geschaffen. Gerade diesem Ziel dienen die als Bestandteil jeder Beurteilungsaktion nicht wegzudenkenden Gremiumsbesprechungen, an denen alle Vorgesetzten, die mit dem betroffenen Personenkreis befaßt sind, teilnehmen. Auf diesem Wege wird eine vergleichende Bewertung erreicht, die dann ein wesentlicher Bestandteil der Beförderungsentscheidungen wird. Im Gesamturteil haben daher die wesentlichen Gesichtspunkte bereits ihren Niederschlag gefunden, so daß die Kritik der Verkürzung der entscheidungserheblichen Fakten fehlgeht.

Zu 7.2.3. Verhaltens- und Leistungskontrolle

Nach Auffassung des Bundesbeauftragten für den Datenschutz unterliegen die Verfahren zur Verhaltens- und Leistungskontrolle mit technischen Systemen der Mitbestimmung. Er hält dabei ein vollständiges Abbild des Arbeitsverhaltens und eine lückenlose Kontrolle der Leistung für unzulässig. Nach seiner Ansicht würden heimliche technische Kontrollen gegen das Recht auf informationelle Selbstbestimmung verstoßen. Der Bundesbeauftragte für den Datenschutz regt deshalb an, bei der Entwicklung derartiger Systeme vorrangig eine konventionelle Dienstaufsicht vor maschineller Kontrolle zu berücksichtigen. Außerdem

sollte dem Betroffenen aus Transparenzgründen der Kontrollzeitraum mitgeteilt werden. Kontrollen sollen nur stichprobenweise und aus konkretem Anlaß erfolgen und individuelle Kontrollen erst dann, wenn solche mit nicht personenbezogenen Daten wirkungslos sind.

Der Bundesminister für das Post- und Fernmeldewesen bemerkt hierzu: Die Deutsche Bundespost mißt dem Abschluß einer Dienstvereinbarung mit dem Hauptpersonalrat gemäß §§ 73, 75 Abs. 3 Nr. 17 BPersVG höchste Priorität bei. Die anderslautende Darstellung des Bundesbeauftragten für den Datenschutz im vorletzten Absatz trifft nicht zu. Seine Wiedergabe der Antwort des Bundesministers für das Post- und Fernmeldewesen, „eine nur stichprobenweise Kontrolle sei aus datenschutzrechtlichen Gründen nicht geboten", ist unrichtig und von der Deutschen Bundespost nicht gegeben worden.

Der Bundesbeauftragte für den Datenschutz ist offensichtlich der Meinung, daß eine Leistungs- oder Verhaltenskontrolle der Beschäftigten aus datenschutzrechtlichen Gründen, wenn überhaupt, dann nur in dem von ihm aufgezeigten engen Rahmen zulässig ist. Diese Auffassung wird von der Deutschen Bundespost nicht geteilt. Sie ist vielmehr der Auffassung, daß sie auch aus Gründen sparsamer Haushaltsführung verpflichtet ist, eine Fachaufsicht auszuüben, ob und wie bezahlte Leistungen erbracht werden. Sie entscheidet in alleiniger Zuständigkeit, in welcher Weise und in welchem Umfang sie die Kontrollen unter Beachtung der Gesetze und der Rechtsprechung vornimmt. Die Bestimmungen des Bundesdatenschutzgesetzes (insbesondere § 7 Abs. 3 i. V. m. § 23 BDSG) bleiben hiervon unberührt. Die Deutsche Bundespost weiß sich insoweit in Übereinstimmung mit der Rechtsprechung des Bundesarbeitsgerichts (vgl. zuletzt: BAG — 1 ABR 48/84 — vom 27. Mai 1986).

Die Deutsche Bundespost legt Wert darauf, daß der Bundesbeauftragte für den Datenschutz sich nur an die im Bundesdatenschutzgesetz als Normadressaten genannten Behörden und sonstigen öffentlichen Stellen wendet. Dies schließt einen direkten Zugang des Bundesbeauftragten für den Datenschutz zu den Personalvertretungen bei den Behörden aus, da Personalvertretungen keine selbständigen Behörden oder sonstige öffentliche Stellen sind.

Zu 8. Deutsche Bundespost

Zu 8.1. Probleme der Zusammenarbeit mit dem Bundesministerium für das Post- und Fernmeldewesen

Zur Zusammenarbeit mit dem Bundesministerium für das Post- und Fernmeldewesen führt der Bundesbeauftragte für den Datenschutz aus, daß diese sich in einigen Bereichen positiv, in anderen Bereichen wesentlich schwieriger gestalte. Es führe zu einer erheblichen Belastung des Bundesbeauftragten für den Datenschutz, daß die Bearbeitung der Stellungnahmen durch den Bundesminister für das Post- und Fernmeldewesen oft mehrere Monate dauere. Nach Meinung des Bundesbeauftragten für den Datenschutz wäre eine Beschleunigung erreichbar, wenn er sich direkt an die nachgeordnete Behörde wenden könnte. Außerdem beklagt er, daß die Deutsche Bundespost ihn über die bevorstehende Einführung neuer datenschutzrelevanter Dienstleistungen nicht oder erst sehr spät informiere und der Bundesminister für das Post- und Fernmeldewesen darauf verweise, daß für ihn eine Verpflichtung zur Inanspruchnahme von Beratungen durch den Bundesbeauftragten für den Datenschutz nicht bestehe.

Zu den beiden vom Bundesbeauftragten für den Datenschutz angesprochenen Problembereichen führt der Bundesminister für das Post- und Fernmeldewesen aus:

1. Der Bundesminister für das Post- und Fernmeldewesen ist bemüht, die Bearbeitungsdauer der einzelnen Vorgänge in einem vertretbaren Zeitrahmen zu halten. Bedingt durch den dreistufigen Behördenaufbau der Deutschen Bundespost (Amtsebene, Direktionsebene und Ministerium) werden zur Ermittlung des zutreffenden Sachverhalts oftmals Rückfragen des Ministeriums bei den nachgeordneten Behörden erforderlich, die häufiger zeitliche Verzögerungen zur Folge haben. Erst aufgrund der vorgelegten Berichte kann das Ministerium feststellen, ob nur in einem Einzelfall gegen bestehende Vorschriften verstoßen wurde oder ob in Fragen grundsätzlicher Art Konsequenzen für den Bereich der gesamten Deutschen Bundespost zu ziehen sind. Bei der derzeitigen Verfahrensweise wird auch der Gefahr vorgebeugt, daß aus einem Verstoß bei einer einzelnen Behörde — was sich bei dem Massenbetrieb einer Betriebsverwaltung wie der Deutschen Bundespost nicht ganz ausschließen läßt — verallgemeinernd auf ein fehlerhaftes Verfahren bei der Deutschen Bundespost insgesamt geschlossen wird. Zum Vorschlag des Bundesbeauftragten für den Datenschutz, sich zur Verfahrensbeschleunigung direkt an die zuständige Postbehörde zu wenden, ist festzustellen, daß der Bundesminister für das Post- und Fernmeldewesen im Informationsaustausch mit einbezogen bleiben muß, damit er die Möglichkeit hat, im Rahmen seiner Dienst- und Fachaufsicht ggf. nachzusteuern. Aus den angeführten Gründen wird die vom Bundesbeauftragten für den Datenschutz angeregte Verfahrensänderung nicht für zweckmäßig erachtet und im Ergebnis abgelehnt. Gleichwohl wird die Deutsche Bundespost auch künftig bemüht bleiben, die Bearbeitungsdauer zu beschleunigen und vermehrt von der Möglichkeit der Erteilung von Zwischenbescheiden Gebrauch zu machen.

   Eine Entlastung des Bundesbeauftragten für den Datenschutz scheint u. U. dadurch möglich zu sein, indem er die von Bürgern vorgetragenen Beschwerden, die offensichtlich in keinem Zusammenhang mit einer Speicherung personenbezogener Daten bei Behörden der Deutschen Bundespost stehen, beispielsweise bei Sendungsverlusten, Falschzustellungen oder behaupteten Verletzungen des Fernmeldegeheimnisses, der Deutschen Bundespost zuständigkeitshalber zur Erledigung übersendet.

2. Die Deutsche Bundespost ist grundsätzlich bemüht, den Bundesbeauftragten für den Datenschutz bei der Einführung neuer DV-gestützter Dienste nach Möglichkeit so frühzeitig zu beteiligen, daß er hinreichend Gelegenheit hat, noch vor Einführung neuer Dienste Empfehlungen zur Gewährleistung des Datenschutzes zu geben. Eine ausnahmslose Beteiligung bei allen datenschutzrechtlich relevanten Verwaltungsvorgängen unabhängig von der Bedeutung der Maßnahme und dem erreichten Konkretisierungsgrad ist jedoch weder rechtlich geboten noch verwaltungstechnisch überhaupt möglich.

Zu 8.2. Telekommunikationsordnung

Der Bundesbeauftragte für den Datenschutz bedauert, daß ihm der Entwurf der „Verordnung über die Bedingungen und Gebühren für die Benutzung der Einrichtungen des Fernmeldewesens (Telekommunikationsordnung — TKO)" erst recht spät zugänglich gemacht wurde. Der Bundesbeauftragte für den Datenschutz hat den Bundesminister für das Post- und Fernmeldewesen daraufhin auf einige aus seiner Sicht besonders wichtige datenschutzrechtliche Probleme bzw. Defizite hingewiesen und Änderungen und Ergänzungen angeregt. Der Bundesbeauftragte für den Datenschutz bemängelt, daß der Verwaltungsrat der Deutschen Bundespost die TKO verabschiedet hat, ohne seine Anregungen aufzugreifen.

Der Bundesminister für das Post- und Fernmeldewesen stellt hierzu fest, daß die Mitglieder des Verwaltungsrates der Deutschen Bundespost ihre Stellung nach dem Prinzip des freien Mandats ausüben. Die Mitglieder sind an keine Aufträge oder Weisungen gebunden. Sie haben ihr Amt gemäß § 5 Abs. 3 Postverwaltungsgesetz (PostVwG) nach bestem Wissen und Gewissen auszuüben.

Der Entwurf der TKO ist dem Bundesbeauftragten für den Datenschutz unmittelbar nach Fertigstellung am 4. Dezember 1985 — gleichzeitig mit der Zusendung an den Verwaltungsrat — und damit nicht verspätet, sondern so frühzeitig wie möglich zur Kenntnis gebracht worden. Bis zur Beschlußfassung der TKO im Verwaltungsrat am 30. Juni 1986 standen dem Bundesbeauftragten für den Datenschutz demnach mehrere Monate zur Prüfung, Meinungsbildung und Diskussion mit der Deutschen Bundespost zur Verfügung. Richtig ist, daß die mit dem Bundesbeauftragten für den Datenschutz intensiv geführten Gespräche auf der Fachebene (24. bis 26. März 1987) und der Leitungsebene (21. Mai 1986) nicht zur Übereinstimmung in allen datenschutzrechtlich relevanten Fragen geführt haben.

Zu den vom Bundesbeauftragten für den Datenschutz bemängelten fünf Punkten, die auch Gegenstand ausführlicher Beratung im Verwaltungsrat der Deutschen Bundespost waren — der Brief des Bundesbeauftragten für den Datenschutz vom 23. Juni 1986 an den Vorsitzer hat den Mitgliedern vorgelegen — und von denen die ersten drei Punkte bereits im Achten Tätigkeitsbericht genannt waren, führt der Bundesminister für das Post- und Fernmeldewesen aus:

1. Tragfähigkeit der Verordnungsermächtigung

Auf der Basis des Berichts der Regierungskommission Fernmeldewesen wird die Bundesregierung in dieser Legislaturperiode über eine Neustrukturierung des Post- und Fernmeldewesens entscheiden.

In diesem Rahmen ist eine Novellierung des Postverwaltungsgesetzes, die den § 14 einschließt, erforderlich.

Die Bundesregierung wird einen entsprechenden Gesetzentwurf so rechtzeitig vorlegen, daß er noch in dieser Legislaturperiode verabschiedet werden kann.

2. Grundsatz der Eintragung aller Fernsprechteilnehmer

In der rechtlichen Bewertung des Bucheintrags der Telefonteilnehmer bestehen zwar nach wie vor unterschiedliche Auffassungen hinsichtlich der Frage, ob die Deutsche Bundespost mit der Eintragung zwangsweise in Grundrechtspositionen eingreift. Die Standpunkte haben sich jedoch insofern angenähert, als der Bundesbeauftragte für den Datenschutz aufgrund der vorgetragenen Argumente der Deutschen Bundespost nunmehr anerkennt, daß die Eintragung möglichst aller Teilnehmer „in mehrfacher Hinsicht wünschenswert erscheint". Daher überrascht, daß der Bundesbeauftragte für den Datenschutz dennoch nicht akzeptiert, daß der Grundsatz der Eintragung solcher Teilnehmer, die keinen vernünftigen Sachgrund für den Nichteintrag nennen können, im überwiegenden Allgemeininteresse liegt. Wenn nämlich eine erhebliche Zahl von Teilnehmern nicht im Telefonbuch verzeichnet wäre, würde das private und geschäftliche Zusammenleben voraussichtlich stark beeinträchtigt. Auch würden weitgehend lückenhafte Fernsprechverzeichnisse in nicht vertretbarer Weise den ohnehin schon stark defizitären Auskunftsdienst der Deutschen Bundespost noch mehr, und zwar zum Nachteil aller Teilnehmer, belasten. Hinzu kommt, daß eingetragene Fernsprechteilnehmer vermehrt durch Anrufe belästigt würden, die für nicht eingetragene Teilnehmer gleichen Namens bestimmt sind. Die Deutsche Bundespost hält daher nach wie vor die benutzungsrechtlich insgesamt großzügig gestaltete Regelung des Bucheintrags für rechtmäßig und sachlich begründet. Dem entspricht, daß bisher auch alle insoweit ergangenen Gerichtsurteile die Eintragungspraxis der Deutschen Bundespost als rechtmäßig anerkannt haben. Auch der Petitionsausschuß des Deutschen Bundestages hat die Gründe der Deutschen Bundespost, am Grundsatz des Pflichteintrags festzuhalten, ausdrücklich als plausibel anerkannt.

3. Registrierung von Verbindungsdaten von Telefongesprächen bei belästigenden Anrufen

Das Problem, unter welchen Voraussetzungen Verbindungsdaten auf Antrag des Teilnehmers bei belästigenden Anrufen sowie zur Kontrolle der Gebührenberechnung festgehalten und an den Teilnehmer her-

ausgegeben werden dürfen, ist nunmehr entsprechend den Ergebnissen der Besprechungen mit dem Bundesbeauftragten für den Datenschutz in der TKO (§§ 84, 453) vollständig und präzise geregelt. Angesichts des Umfangs und der Kompliziertheit der Regelung stellt sich jedoch die Frage, ob auf diese Weise das eigentliche Ziel, dem Teilnehmer mehr Transparenz zu vermitteln, tatsächlich erreicht werden kann.

4. Registrierung von Ausweisdaten

In der Vergangenheit ist es in Einzelfällen vorgekommen, daß im Interesse der Durchsetzung rückständiger Gebührenforderungen von ausländischen Schuldnern beim Antrag auf Einrichtung eines Fernsprechhauptanschlusses Ausweisdaten festgehalten wurden. Die Deutsche Bundespost hat sich nunmehr aufgrund erneuter Prüfung entschlossen, zukünftig auf die Registrierung solcher Ausweisdaten beim Antrag auf Einrichtung eines Telefons zu verzichten.

5. Datenregistrierung im Funkfernsprechdienst

Die vom Bundesbeauftragten für den Datenschutz angesprochene Registrierung der Verbindungsdaten im Funkfernsprechdienst ist aufgrund der zur Zeit noch gegebenen technischen Bedingungen unverzichtbar, um die mißbräuchliche Verwendung von Teilnehmerkennungen in diesem Bereich zu verhindern bzw. aufzudecken sowie den Teilnehmer vor unberechtigten Gebührenforderungen zu schützen. Für die Praxis geeignete Alternativen, die den Verzicht auf die Vollspeicherung von Verbindungsdaten rechtfertigen könnten, sind auch vom Bundesbeauftragten für den Datenschutz bisher nicht aufgezeigt worden. Eine ausdrückliche Regelung in der TKO ist nach Auffassung der Deutschen Bundespost nicht erforderlich, da mit der beabsichtigten Einführung einer Chipkarte etwa im Jahre 1989 aller Voraussicht nach ein Mißbrauch fremder Teilnehmerkennungen nicht mehr gegeben sein wird. Hinzu kommt, daß bereits § 388 TKO die Speicherung von Verbindungsdaten zur Mißbrauchsverhinderung ausdrücklich erlaubt.

Zu 8.3. Bekanntgabe der Daten von Kabel- bzw. Satellitenfunkteilnehmern

Der Bundesbeauftragte für den Datenschutz wie auch der Bayerische Landesbeauftragte für den Datenschutz machen nunmehr Bedenken hinsichtlich des Anspruchs der Bayerischen Landeszentrale für neue Medien (BLM) auf Übermittlung personenbezogener Daten bei fernmelderechtlichen Genehmigungen zum Betrieb von Satellitenempfangsanlagen durch die Deutsche Bundespost für den Fall geltend, daß diese nicht der Weiterverbreitung, sondern ausschließlich der Eigenversorgung mit Rundfunkprogrammen (Individualempfang oder Demonstrationszwecke) dienen. Da hier keine Weiterverbreitung von Rundfunkprogrammen im Sinne des Bayerischen Medienerprobungs- und -entwicklungsgesetzes (MEG) vorliege, sei mangels rundfunkrechtlichen Genehmigungserfordernisses nach § 35 Abs. 1 Satz 2 MEG ein Tätigwerden der BLM nicht veranlaßt. Eine Übermittlung personenbezogener Daten dieser Inhaber einer fernmelderechtlichen Genehmigung durch die Deutsche Bundespost an die BLM ohne deren Einwilligung sei mithin unzulässig.

Der Bundesminister für das Post- und Fernmeldewesen bemerkt hierzu: Genehmigt die Deutsche Bundespost einem Antragsteller den Betrieb einer Satellitenempfangsanlage, so wird die BLM hierüber unterrichtet. Diese Information erfolgt im Wege der Amtshilfe gemäß § 10 Abs. 1 Satz 1 Alternative 2 BDSG aufgrund ausdrücklicher Anforderung der BLM. Bei der Prüfung der generellen Zulässigkeit der Datenübermittlung war für die Deutsche Bundespost entscheidend, daß nach dem MEG die Aufgaben, für die die Angaben von der Deutschen Bundespost verlangt werden, generell in die Zuständigkeit der BLM fallen und die BLM der Deutschen Bundespost gegenüber erklärt hat, daß der Bayerische Datenschutzbeauftragte keine Einwände gegen den Anspruch der BLM geltend mache, neben der rundfunkrechtlichen Genehmigung auch Unbedenklichkeitsbescheinigungen in den Fällen zu erteilen, in denen eine Genehmigung nach § 35 MEG nicht erforderlich ist.

Da sich die Frage der Zulässigkeit der Datenübermittlung bei bloßen Individualanlagen vorrangig danach richtet, ob nach bayerischem Landesrecht der rechtmäßige Betrieb auch solcher Anlagen von einer rundfunkrechtlichen „Unbedenklichkeitsbescheinigung" abhängig gemacht werden kann, erscheint es zweckmäßig, vor einer abschließenden Entscheidung über die Zulässigkeit der Datenübermittlung durch die Deutsche Bundespost zunächst die vom Bayerischen Datenschutzbeauftragten wie auch von der BLM gemeinsam angestrebte Klärung dieser landesrechtlichen Frage abzuwarten. Dies gilt um so mehr, als nach dem derzeitigen Erkenntnisstand im Rahmen der Novellierung des MEG die Frage abschließend entschieden werden soll, ob die Nutzung der privaten Satellitenempfangsanlagen nur für eigene Zwecke von einer rundfunkrechtlichen Unbedenklichkeitsbescheinigung abhängig sein soll.

Zu 8.4. Kabelpilotprojekt Dortmund

Nach den Feststellungen des Bundesbeauftragten für den Datenschutz hat die Datenschutzkontrolle des Kabelpilotprojekts Dortmund keine Anhaltspunkte für eine Registrierung des „Fernsehverhaltens" der angeschlossenen Teilnehmer durch die Deutsche Bundespost ergeben. Der Bundesbeauftragte für den Datenschutz beanstandet, daß die Teilnehmerdatei weder veröffentlicht noch zum Register angemeldet worden ist. Er kritisiert die fehlende Transparenz des für die Antragstellung verwendeten Formblatts. Bei den Datenübermittlungen an den Kabelfunk Dortmund, den Handwerksbetrieb (Pilotkabelgemeinschaft) und insbesondere an die Handwerkskammern werde dem Grundsatz der Erforderlichkeit nicht immer durchgängig Rechnung getragen. Der Bundesbeauftragte für den Datenschutz schlägt zudem Verbesserungen

der technisch-organisatorischen Sicherheitsmaßnahmen vor.

Der Bundesminister für das Post- und Fernmeldewesen führt hierzu aus: Die Deutsche Bundespost legt großen Wert darauf, daß ihre Dienststellen nicht nur das verfassungsrechtlich geschützte Fernmeldegeheimnis strikt einhalten, sondern auch schon bei der Planung neuer Fernmeldedienste und fernmeldetechnischer Systeme die berechtigten datenschutzrechtlichen Belange der Teilnehmer berücksichtigen. Die Dienststellen der Deutschen Bundespost speichern in den technischen Einrichtungen daher nur die personenbezogenen Daten, die zur Erfüllung ihrer Aufgaben erforderlich sind. Schon dadurch wird verhindert, daß im Zusammenwirken verschiedener Dateien Persönlichkeitsprofile erstellt werden können.

Das Fernmeldeamt Dortmund 1 hatte als speichernde Stelle die Veröffentlichung und die Anmeldung der Datei „Pilotprojektdatei (FAT-System)" versehentlich nicht veranlaßt. Dies wurde jedoch nachgeholt. Die „Übersicht über die Art der gespeicherten personenbezogenen Daten" wurde ergänzt.

Das Formblatt „Antrag auf Kabelanschluß und Teilnahme am Kabelpilotprojekt Dortmund" wurde geändert. Die Anregungen des Bundesbeauftragten für den Datenschutz wurden eingearbeitet. Der Antragsteller kann nun genau erkennen, welche Angaben er machen muß, damit die Deutsche Bundespost die beantragte Dienstleistung erbringen kann, und welche er darüber hinaus freiwillig abgeben kann.

Die Übermittlung der Daten des Antragstellers an den Kabelfunk Dortmund ist nach § 10 Abs. 1 Satz 1, Alternative 2, BDSG zulässig, denn sie ist zur rechtmäßigen Aufgabenerfüllung des Empfängers, nämlich der Abrechnung der Rundfunkgebühren, erforderlich. Die Telefonnummer des Antragstellers wird dazu jedoch nicht benötigt; sie wird daher nicht mehr weitergegeben. Darauf wird der Teilnehmer im neuen Antragsvordruck auch ausdrücklich hingewiesen.

An einen fachkundigen Handwerksbetrieb wurden die personenbezogenen Daten des Antragstellers bislang nur dann weitergegeben, wenn der Betroffene schriftlich eingewilligt hatte. Der Antragsteller gab die Einwilligungserklärung auf dem Antragsformblatt zusammen mit anderen Erklärungen ab. Er konnte dabei das Kästchen „einverstanden" oder „nicht einverstanden" ankreuzen. Damit war sichergestellt, daß er die Einwilligung von den anderen Erklärungen hinreichend deutlich unterscheiden und sich mit ihr getrennt beschäftigen konnte (§ 3 BDSG). Seit dem 1. Dezember 1986 werden wegen Wegfalls der Zuschüsse des Landes Nordrhein-Westfalen die personenbezogenen Daten an den Handwerksbetrieb nicht mehr übermittelt.

Die Übermittlung personenbezogener Daten in Listenform an die Handwerkskammern wurde eingestellt.

Die Empfehlungen des Bundesbeauftragten für den Datenschutz zur Verbesserung des Schutzes des Rechnersystems durch Zuteilung individueller Paßworte an die Bediensteten anstelle der bislang verwendeten Gruppenpaßworte und die Erhöhung der Mindestwortlänge auf 5 Stellen wurden inzwischen in die betriebliche Praxis umgesetzt. Die Matrix der Zugriffsberechtigungen wurde überprüft. Einem Bediensteten ist jetzt nur noch der Zugriff auf solche Dateien und Verfahren möglich, die zur Durchführung der ihm geschäftsplanmäßig zugewiesenen Aufgaben erforderlich sind. Zudem wurde durch innerdienstliche schriftliche Regelungen einschränkend festgelegt, welcher Mitarbeiter welche Liste mit Teilnehmerdaten ausdrucken lassen kann.

Zu 8.5. Anschriftenermittlung zu posteigener Werbung

Aufgrund der erneut vom Bundesbeauftragten für den Datenschutz vorgebrachten Bedenken wird geprüft, ob die Praxis der Anschriftenermittlung in der Weise umgestellt werden kann, daß zuvor das Einverständnis der Betroffenen eingeholt wird.

Zu 9. Verkehrswesen

Zu 9.2. Verkehrszentralregister

Zu 9.2.1. Stand der Gesetzesvorbereitung

Mit den Vorarbeiten für den Entwurf verbesserter Rechtsvorschriften für das Verkehrszentralregister ist begonnen worden. Ein Teilaspekt, nämlich der Abruf im automatisierten Verfahren aus der Datei der entzogenen Fahrerlaubnisse, ist bereits durch das Gesetz zur Änderung des Straßenverkehrsgesetzes vom 28. Januar 1987 (BGBl. I S. 486) — vgl. 9.1 des Berichts — geregelt worden. Auf die Abhängigkeit zu der geplanten Vollautomatisierung des Verkehrszentralregisters wurde bereits in der Stellungnahme der Bundesregierung zum Siebenten Tätigkeitsbericht hingewiesen.

Zu 9.2.2. Auskunftserteilung nach § 30 StVG (Vollauskunft)

Der Bundesbeauftragte für den Datenschutz fordert eine auf die Erfordernisse des Einzelfalls abgestellte, eingeschränkte Auskunftserteilung aus dem Verkehrszentralregister durch das Kraftfahrt-Bundesamt.

Eine Zwischenbilanz der vom Bundesminister für Verkehr durchgeführten Untersuchungen hat ergeben, daß in den meisten der vom Gesetz genannten Auskunftsfälle eine Vollauskunft unverzichtbar ist. Korrekturen sind allenfalls in Randbereichen möglich (z. B. bei der Ausstellung eines Ersatzführerscheins). Der Bundesminister für Verkehr wird die Ergebnisse mit den Ländern und dem Bundesbeauftragten für den Datenschutz eingehend erörtern. Die Untersuchungen werden mit dem Ziel fortgesetzt, für die beabsichtigte Neufassung der Rechtsvorschriften für das Verkehrszentralregister (vgl. zu 9.2.1) zu angemessenen Auskunftsregelungen zu kommen.

Zu 9.3. Kfz-Zulassungsdaten

Zu 9.3.1. Zusatzerhebung bei Ausländern

Im Zuge der Rechtsangleichung der Straßenverkehrs-Zulassungs-Ordnung an die Neuregelungen im Straßenverkehrsgesetz und in der hierauf beruhenden Fahrzeugregisterverordnung wird sich der Bundesminister für Verkehr um eine Rechtsvereinheitlichung bemühen. Dabei wird auch die vom Bundesbeauftragten für den Datenschutz aufgeworfene Frage zu prüfen sein, ob die Erhebung der Paßdaten und der Heimatanschrift von Ausländern für Maßnahmen nach § 29d StVZO dem Grundsatz der Verhältnismäßigkeit entspricht.

Zu 9.3.2. Übermittlung an die Automobilindustrie

Die Ausführungen des Bundesbeauftragten für den Datenschutz betreffen die (frühere) Übermittlung von Kfz-Zulassungsdaten durch das Kraftfahrt-Bundesamt an die Automobilindustrie. Der Bundesbeauftragte für den Datenschutz legt dar, daß die Übermittlung solcher Daten nur für unmittelbare Zwecke der Verkehrssicherheit (Rückrufaktionen) und unter einschränkenden Bedingungen für statistische Zwecke zulässig sei. Er kritisiert die Möglichkeit der Nutzung solcher Daten durch die Automobilindustrie zur Überwachung der Vertragstreue von Kunden (Großabnehmer und Werksangehörige mit Vorzugskonditionen, die vor Weiterveräußerung der Fahrzeuge Wartezeiten einzuhalten haben). Das Kraftfahrt-Bundesamt habe diese Möglichkeit auch weiterhin nicht in geeigneter Weise unterbunden, nachdem es durch den Bundesminister für Verkehr dazu angewiesen worden sei. In seiner Presseerklärung hat der Bundesbeauftragte für den Datenschutz sogar ausgeführt, das Kraftfahrt-Bundesamt habe solche Daten an die Automobilhersteller weiterhin „zur Vertragskontrolle übermittelt".

Die Darstellung des Bundesbeauftragten für den Datenschutz ist unzutreffend. Nach der im Bericht angeführten Zusatzvereinbarung zwischen dem Kraftfahrt-Bundesamt und den Automobilherstellern, die für die weiteren Übermittlungen nicht anonymisierter Daten jeweils abgeschlossen worden waren, hatten sich die Datenempfänger ausdrücklich verpflichtet, solche Daten nur für Feststellungen zu verwenden, „die zur Erhaltung bzw. Verbesserung der Verkehrssicherheit von Fahrzeugen erforderlich sind", und hatten sich insoweit einer Kontrolle durch das Kraftfahrt-Bundesamt oder Organe der Datenschutzaufsicht unterworfen. Mißbräuchliche Datennutzungen sind dem Kraftfahrt-Bundesamt nicht bekanntgeworden.

Auch der gegen den Bundesminister für Verkehr erhobene Vorwurf, er habe sich nicht um die Unterbindung dieser rechtswidrigen Datenübermittlungen durch das Kraftfahrt-Bundesamt gekümmert, ist unzutreffend. Der Bundesminister für Verkehr hatte das Kraftfahrt-Bundesamt im November 1984 in diesem Zusammenhang unter anderem angewiesen, Einzelheiten der Kontrolle sowie die Frage, welche Daten im einzelnen übermittelt werden sollen, mit dem Bundesbeauftragten für den Datenschutz abzustimmen. Aufgrund eines Schreibens des Bundesbeauftragten vom September 1986 und eines dazu angeforderten Berichts des Kraftfahrt-Bundesamtes vom Oktober 1986 stellte der Bundesminister für Verkehr fest, daß mit dem Bundesbeauftragten für den Datenschutz weiterhin kein volles Einvernehmen über die Art der zu übermittelnden Daten bestand, es insbesondere einen Dissens zum Begriff „Zulassungsdaten" gab. Um über die mögliche und gebotene Begrenzung der Datenübermittlung nach alter Rechtslage Klarheit zu erzielen, hätte es einer erneuten Erörterung und Abstimmung mit dem Bundesbeauftragten für den Datenschutz bedurft. Im Hinblick auf die unmittelbar bevorstehende Verabschiedung und das Inkrafttreten des sog. ZEVIS-Gesetzes (vgl. 9.1 des Berichts), das ohnehin zur einschränkenden Neuordnung derartiger Datenübermittlungen (nur noch für konkrete Rückrufaktionen) führte, hat der Bundesminister für Verkehr dem Bundesbeauftragten für den Datenschutz mit Schreiben vom 26. November 1986 vorgeschlagen, die Entscheidung über das zu Veranlassende bis Anfang 1987 zu vertagen. Dem hat der Bundesbeauftragte für den Datenschutz nicht widersprochen. Das Kraftfahrt-Bundesamt hat schon Mitte Dezember 1986 die betroffenen Automobilhersteller über die sich nach der neuen Gesetzeslage ergebenden Einschränkungen unterrichtet. Die fraglichen Datenübermittlungen wurden mit Ablauf des Januar 1987 eingestellt.

Zu 9.4. Führerschein auf Probe

Die vom Bundesbeauftragten für den Datenschutz angeregten und vom Bundesrat befürworteten Auflagen an den Kursleiter für die Behandlung der Daten über die Teilnehmer der Nachschulkurse sind in § 12d StVZO durch die Verordnung zur Änderung straßenverkehrsrechtlicher Vorschriften vom 31. Dezember 1986 (BGBl. 1987 I S. 80) übernommen worden.

Zu 9.5. Luftfahrt-Bundesamt (LBA)

Zu 9.5.1. Fehlende Rechtsgrundlagen

Der Bundesbeauftragte für den Datenschutz bemängelt das Fehlen einer speziellen gesetzlichen Grundlage für die Übermittlung von Daten der Luftfahrzeugrolle (Angaben über Eigentümer der Luftfahrzeuge) zum Zwecke der Veröffentlichung in den „Nachrichten für Luftfahrer" und im „Registre Aeronautique International". Die vom Bundesbeauftragten für den Datenschutz ursprünglich angezweifelte Notwendigkeit dieser Veröffentlichungen hat der Bundesminister für Verkehr unter Hinweis auf die Interessen der an der Luftfahrt Beteiligten und auch Dritter dargelegt. Zur Zeit wird jedoch geprüft, wie eine hinsichtlich des Datenschutzes und des Volkszählungsurteils nicht zu Zweifeln Anlaß gebende Lösung gefunden werden kann.

Hinsichtlich der ebenfalls angesprochenen Datensammlung für Luftfahrer (Positiv-/Negativdatei) des Luftfahrt-Bundesamtes haben die Luftverkehrsver-

waltungen der Länder zu erkennen gegeben, daß diese Sammlung für sie von hohem Wert im Zusammenhang mit ihrer Zuständigkeit für die Erteilung/Entziehung von Luftfahrerscheinen ist. Notwendigkeit, Rechtsgrundlage und Rechtmäßigkeit dieser Auskunftstätigkeit des Luftfahrt-Bundesamtes sind im übrigen durch einen Beschluß des BVerwG vom 22. Januar 1985 — 7 B 43.84 — grundsätzlich bestätigt worden. Die Überlegungen hinsichtlich einer Präzisierung der Rechtsgrundlagen sind auch auf die Frage einer möglichen Einbeziehung in die geplanten Rechtsvorschriften für das Verkehrszentralregister (vgl. zu 9.2.1) ausgedehnt worden. Der Bundesbeauftragte für den Datenschutz wurde im übrigen darüber informiert, daß eine Einschränkung der Eintragung strafrechtlicher Verurteilungen weder mit dem Zweck der Dateien noch mit § 24 Abs. 2 LuftVZO vereinbar ist.

An der unter 9.5.1. im letzten Absatz angesprochenen inhaltlichen Präzisierung der Regelungen und Rechtsgrundlagen für den Umgang mit den Daten der Flugunfalluntersuchung wird unter Berücksichtigung der Bedenken und Anregungen des Bundesbeauftragten für den Datenschutz intensiv gearbeitet.

Erschwert wird dies durch die unterschiedlichen Interessen der Beteiligten und der um Auskunft Ersuchenden. Gegen die vom Bundesbeauftragten für den Datenschutz geschilderte, bereits vollzogene Einschränkung der Akteneinsicht wurde von Interessenten bereits erfolgreich gerichtlich vorgegangen. Insgesamt stellt sich auch die Frage, ob die Luftunfalluntersuchung zukünftig allein den Empfehlungen der ICAO folgen soll (technische Untersuchung) oder ob sie nicht wegen der unterschiedlichen Interessentenkreise (Staatsanwaltschaft, Luftfahrtbehörde, Versicherungen) in ein dem seeamtlichen ähnliches Verfahren umgestaltet werden kann und muß.

Zu 9.5.2. Technische und organisatorische Mängel

Der Bundesbeauftragte für den Datenschutz bemängelt, daß bei einer Reihe von manuell geführten Karteien mit personenbezogenen Angaben zum Zeitpunkt der Kontrolle Sicherungsmaßnahmen fehlten.

Der Bundesminister für Verkehr bemerkt hierzu, daß die Sicherungsmaßnahmen bei manuellen Karteien des Luftfahrt-Bundesamtes inzwischen entsprechend verbessert wurden. Gleiches gilt für die Paßwortverwaltung für die Datei FLUGAN (Flugunfalluntersuchung).

Bei dieser Datei wird auch das Fehlen der Dokumentation vom Bundesbeauftragten für den Datenschutz bemängelt. Der Bundesminister für Verkehr stellt hierzu fest, daß die Dokumentation für alle neuen sowie die künftigen Programme und Verfahren sichergestellt ist. Nur bei den Alt-Verfahren konnte wegen fehlender Arbeitskapazität die nachträgliche Dokumentation noch nicht verwirklicht werden.

Zu 9.6. Deutsche Bundesbahn (DB)

Zu 9.6.1. Deutsche Bundesbahn als Teilnehmer an Verkehrsverbünden

Der Bundesbeauftragte für den Datenschutz behandelt hier Fragen der Datenerhebung bei Fahrgästen von Verkehrsverbünden, an denen auch die Deutsche Bundesbahn durch ihre Direktionen beteiligt ist. Die Daten werden unter anderem für die Aufteilung der Gesamterlöse auf die an den Verkehrsverbünden beteiligten Verkehrsunternehmen verarbeitet. Der Bundesbeauftragte für den Datenschutz fordert von der Deutschen Bundesbahn ein einheitliches Vorgehen ihrer Direktionen sowie ein Hinwirken in den Verbünden auf eine Verwendung möglichst nur anonymisierter Daten, evtl. durch Erhebung der Daten bei den Fahrgästen lediglich unter Angabe der Verbundpaßnummer.

Zu den im Bericht genannten Einzelheiten der Anonymisierung hat die Deutsche Bundesbahn inzwischen gegenüber dem Bundesbeauftragten für den Datenschutz Stellung genommen. Wie sie gegenüber dem Bundesminister für Verkehr erklärt hat, bleibt sie im übrigen weiterhin bemüht, die Abrechnung zwischen den Verbundpartnern und die korrekte Erlöszuteilung auf die einzelnen Gesellschafter auf der Grundlage anonymer statistischer Erhebungen durchzuführen und in den Tarifverbünden auf dieses Ziel hinzuwirken.

Zu 10. Statistik

Zu 10.5. Handels- und Gaststättenzählung und Steuergeheimnis

Der Bundesbeauftragte für den Datenschutz ist der Meinung, daß die Übermittlung der Steuer- und Finanzamtnummer der im Rahmen dieser Zählung von der Erhebung betroffenen Unternehmen durch die Finanzbehörden an die statistischen Landesämter gegen das Steuergeheimnis nach § 30 Abgabenordnung (AO) verstößt.

Der Bundesminister der Finanzen stellt hierzu fest, daß durch die Übermittlung der Steuernummer an die statistischen Landesämter bei der Handels- und Gaststättenzählung 1985 die Finanzbehörden nicht gegen die Pflicht zur Wahrung des Steuergeheimnisses verstoßen haben. Zwar schützt § 30 AO bereits die Tatsache, daß sich eine bestimmte Finanzbehörde mit einem bestimmten Steuerpflichtigen befaßt, was auch in der Vergabe einer Steuernummer zum Ausdruck kommt. Jedoch stellt die Übermittlung der Steuernummern im konkreten Fall keine Offenbarung im Sinne des § 30 AO dar. Eine Offenbarung nach dieser Vorschrift setzt voraus, daß das, was offenbart wird, nicht offenkundig und auch dem Empfänger der Mitteilung noch nicht bekannt ist. Bei der Handels- und Gaststättenzählung wurden den statistischen Landesämtern die Anschriften der Steuerpflichtigen mitgeteilt. Bereits durch diese im Handelsstatistikgesetz ausdrücklich zugelassene Datenübermittlung wurden den statistischen Landesämtern bekannt, daß die be-

troffenen Steuerpflichtigen steuerlich erfaßt sind. Die Übermittlung der Steuernummern brachte deshalb den statistischen Landesämtern insoweit keine neuen Erkenntnisse. Ihnen wurde nichts im Sinne des § 30 AO offenbart.

Die Übermittlung der Steuernummern war auch nicht deshalb unzulässig, weil durch sie nach Auffassung des Bundesbeauftragten für den Datenschutz die Verknüpfung der übermittelten Daten mit anderen, bereits bei den statistischen Landesämtern vorhandenen Daten ermöglicht worden sei. Steuernummern sind als statistische Hilfsmerkmale — wie im vorliegenden Fall auch geschehen — nach Zweckerfüllung zu löschen. Darüber hinaus gilt für die statistischen Ämter die Pflicht zur Wahrung des Steuergeheimnisses. Das Steuergeheimnis ist auch innerhalb dieser Ämter zu wahren. Bei Beachtung der gesetzlichen Bestimmungen ist deshalb eine Verknüpfung verschiedener Daten bei den statistischen Landesämtern mit Hilfe der Steuernummer nicht möglich.

Zu 11. Sozialwesen

Der Bundesbeauftragte für den Datenschutz bezweifelt, daß der im Bundesministerium für Arbeit und Sozialordnung erarbeitete Entwurf eines Gesetzes zur Regelung der Verwendung der Versicherungsnummer auch die Verwendung der Nummer durch die Arbeitsmedizinischen Dienste der Bau-Berufsgenossenschaften rechtfertigt.

Die Arbeitsmedizinischen Dienste der Bau-Berufsgenossenschaften seien — anders als der Entwurf voraussetzt — möglicherweise keine gesetzliche Aufgabe der Berufsgenossenschaften nach dem Sozialgesetzbuch, sondern deren gesetzliche Aufgabe nach dem Arbeitssicherheitsgesetz.

Hierzu äußert sich der Bundesminister für Arbeit und Sozialordnung wie folgt:

Die Berufsgenossenschaften haben nach § 546 Abs. 1 RVO mit allen geeigneten Mitteln für die Verhütung von Arbeitsunfällen und Berufskrankheiten zu sorgen.

Eines dieser Mittel ist — wie die Verweisung von § 546 Abs. 2 RVO auf § 719a RVO ergibt — auch die Einrichtung und der Betrieb überbetrieblicher arbeitsmedizinischer Dienste. Im Rahmen solcher Verhütung von Arbeitsunfällen und Berufskrankheiten können sie auch die Versicherungsnummer der gesetzlichen Rentenversicherung erheben und verwenden.

Die jahrelangen Auseinandersetzungen um die Auslegung des § 9 Abs. 2 BDSG zwischen dem Bundesbeauftragten für den Datenschutz einerseits und den Spitzenverbänden der Sozialversicherung andererseits haben den Bundesminister für Arbeit und Sozialordnung veranlaßt, einen „Entwurf von Hinweisen über die Berücksichtigung datenschutzrechtlicher Gesichtspunkte in Vordrucken und Merkblättern" zu erstellen und mit dem Bundesbeauftragten für den Datenschutz und den Spitzenverbänden der Sozialversicherung in den Grundzügen abzustimmen. Dieser Entwurf bedarf — nach der zu erwartenden Novellierung des Bundesdatenschutzgesetzes — nochmals der Feinabstimmung. Es besteht die Hoffnung, daß er dann, z. B. in einem gemeinsamen Rundschreiben der Spitzenverbände, festgeschrieben und — soweit noch erforderlich — in die Formulare der Leistungsträger umgesetzt werden kann. Im Bereich der sozialen Sicherung herrscht die Meinung vor, daß im allgemeinen die Umsetzung des § 9 Abs. 2 BDSG in die Praxis bereits gelungen sei. Der Bundesminister für Arbeit und Sozialordnung hat deshalb den Bundesbeauftragten für den Datenschutz gebeten, Vordrucke und Merkblätter, die er als fehlerhaft ansieht, dem Bundesminister für Arbeit und Sozialordnung zur Verfügung zu stellen.

Zu 11.1. Arbeitsverwaltung

Zu 11.1.1. Arbeitsvermittlung/-beratung

Der Bundesbeauftragte für den Datenschutz vertritt die Auffassung, für die Arbeitsvermittlung (§§ 13, 14 AFG) seien im Sinne des § 69 Abs. 1 Nr. 1 SGB X nur der Name, die Anschrift, gegebenenfalls die Telefonnummer sowie die Bezeichnung der beruflichen Qualifikation des Arbeitsuchenden erforderlich. Dann könne der potentielle Arbeitgeber mit dem Arbeitsuchenden von sich aus in Kontakt treten. Die Übermittlung weiterer Daten sei nur auf Grund der Einwilligung des Betroffenen (§ 67 Abs. 1 SGB X) zulässig.

Die Bundesregierung hält die Einwendungen für nicht begründet. Insbesondere ist nicht zu erkennen, auf welchen Kenntnissen und Erfahrungen die Feststellung beruht, daß für eine erfolgreiche Arbeitsvermittlung der Name, die Anschrift und ggf. die Telefonnummer sowie die Bezeichnung der beruflichen Qualifikation ausreichen und die Weiterleitung von Bewerbungsunterlagen fachlich nicht erforderlich ist.

Die Vorlage von Bewerbungsunterlagen, die die Arbeitsämter von Arbeitsuchenden zum Zwecke der Arbeitsvermittlung erhalten, ist durch die §§ 13, 14 und 22 AFG gedeckt und seit jeher ein fester Bestandteil der Vermittlungstätigkeit der Arbeitsämter, die auf den Nutzen des Arbeitsuchenden ausgerichtet ist und zu diesem Zweck berechtigte Forderungen der Arbeitgeber zu berücksichtigen hat. Die Arbeitsämter würden ihrer gesetzlichen Aufgabe nicht entsprechen, wenn sie die Chancen der Arbeitsuchenden auf einen Arbeitsplatz dadurch einschränkten, daß sie dem im Bereich der Angestelltenberufe, vielfach aber auch bei Facharbeitern, üblichen Verlangen der Arbeitgeber nicht nachkämen, Bewerbungsunterlagen der zur Einstellung vorgeschlagenen Arbeitsuchenden vorzulegen.

Die Weiterleitung der Bewerbungsunterlagen ist daher nach § 69 Abs. 1 Nr. 1 SGB X zulässig. Die Bundesanstalt für Arbeit wird in einer Informationsbroschüre für Arbeitsuchende und Arbeitgeber diese Rechtslage ausführlich erläutern und hierauf auch in den „Hinweisen zum Ausfüllen der Beratungs- und Vermittlungsunterlage" eingehen. Dabei werden die Arbeitsuchenden ausdrücklich auch darauf hingewiesen, daß sie die Weiterleitung von Bewerbungsunterlagen allgemein oder an bestimmte Arbeitgeber von

ihrer vorherigen Zustimmung abhängig machen können. Die Arbeitsuchenden erhalten Gelegenheit, ihre Entscheidung in einfacher Form vordruckmäßig mitzuteilen.

Für die Vermittlung von Bewerbern zu internationalen Organisationen gilt gegenüber den allgemeinen Vermittlungsverfahren nur die Besonderheit, daß das Arbeitsamt die Daten des Bewerbers nicht unmittelbar der internationalen Organisation zuleitet, sondern an das zuständige Bundesministerium zur Benennung eines deutschen Bewerbers gegenüber der internationalen Organisation gibt. Diese Weiterleitung an das Ministerium ist gleichfalls im Sinne des § 69 Abs. 1 Nr. 1 SGB X erforderlich, weil ohne Unterstützung durch das zuständige Ressort zu internationalen Organisationen nicht mit Aussicht auf Erfolg vermittelt werden kann.

Die Einschaltung des zuständigen Bundesministeriums ist den Bewerbern bekannt. Unter anderem weisen die von der Bundesanstalt für Arbeit herausgegebenen Blätter zur Berufskunde „Beamter/Beamtin bei internationalen Organisationen" und „Die Mitarbeit von Deutschen in internationalen Organisationen" darauf hin. Im übrigen soll in die einschlägigen Formschreiben und Vordrucke der Bundesanstalt für Arbeit ein Hinweis auf die Einschaltung des zuständigen Bundesministeriums im Rahmen des Vermittlungsverfahrens aufgenommen werden.

Zu 11.1.2. Leistungsverwaltung

Der Bundesbeauftragte für den Datenschutz strebt nunmehr eine Rechtsänderung an, durch die in Anlehnung an die Regelung des § 50 Abs. 2 Satz 3 Bundesausbildungsförderungsgesetz im Bescheid über die Bewilligung oder Ablehnung von Arbeitslosenhilfe die Angaben über das Einkommen des Unterhaltspflichtigen abweichend von § 35 Abs. 1 SGB X dann unter bestimmten Voraussetzungen entfallen können, wenn ein Unterhaltsverpflichteter dies unter Angaben von Gründen verlangt.

Die Bundesregierung hält an ihrer in der Stellungnahme zum Achten Tätigkeitsbericht (zu 10.4) dargestellten Rechtsauffassung fest. Das Interesse des Arbeitslosen an der Überprüfung der Rechtmäßigkeit eines ihn belastenden Verwaltungsaktes hat grundsätzlich Vorrang vor dem Interesse des Unterhaltsverpflichteten an der Geheimhaltung seiner Einkommensverhältnisse. Sie wird jedoch prüfen, ob es Fälle gibt, in denen auf die Angaben der Einkommensverhältnisse des Unterhaltsverpflichteten im Bescheid über die Bewilligung oder Ablehnung von Arbeitslosenhilfe zunächst verzichtet werden kann, weil ein Überprüfungsinteresse des Arbeitslosen nicht besteht.

Der Bundesbeauftragte für den Datenschutz bemängelt, daß die Bundesanstalt für Arbeit dem Sozialgericht auf Anforderung die Leistungsakten einschließlich der ärztlichen Gutachten übersendet. Er ist der Auffassung, das in § 76 Abs. 2 Satz 2 SGB X festgelegte Widerspruchsrecht des Betroffenen gegen die Überlassung des Gutachtens gelte auch gegenüber dem Sozialgericht und erfordere es, den Betroffenen auf sein Widerspruchsrecht aufmerksam zu machen.

Die Bundesregierung geht demgegenüber davon aus, daß das Sozialgesetzbuch die Übermittlung der ganzen Akte einschließlich des ärztlichen Gutachtens an das Gericht nach § 69 Abs. 1 Nr. 1 und § 76 Abs. 1 SGB X gestattet, ohne daß es auf den Ausnahmetatbestand des § 76 Abs. 2 SGB X und den dort vorgesehenen Widerspruch des Betroffenen ankommt.

Bei der Beurteilung, was für die Durchführung eines mit der gesetzlichen Aufgabe des Leistungsträgers zusammenhängenden gerichtlichen Verfahrens (§ 69 Abs. 1 Nr. 1 2. Alternative SGB X) erforderlich ist, kommt es dabei auf die Auffassung des Gerichts und nicht des Leistungsträgers oder des Betroffenen an (Hauck-Haines-Walloth zu § 69 SGB X, Rdnr. 27), weil sonst die gerichtliche Kontrolle der Leistungsträger unterlaufen würde.

§ 76 Abs. 1 SGB X läßt als zusätzliche Sperre die Offenbarung dem Leistungsträger von einem Arzt überlassener Daten nur unter den Voraussetzungen zu, unter denen der Arzt selbst offenbarungsbefugt wäre. Damit ist gemeint, daß für den Leistungsträger ein Rechtfertigungsgrund vorliegen muß, der seiner Art nach auch dem Arzt bei der Offenbarung dem Arztgeheimnis unterliegender Daten (im Rahmen des § 203 StGB) zur Seite steht. Als solche Rechtfertigungsgründe kommen Einwilligung, mutmaßliche Einwilligung, gesetzliche Mitteilungspflichten, Wahrnehmung berechtigter Interessen und rechtfertigender Notstand in Betracht.

In dem vom Bundesbeauftragten für den Datenschutz genannten Fall greift der Rechtfertigungsgrund der Wahrnehmung berechtigter Interessen. Im Rechtsstreit zwischen Arzt und Patient dürfte auch der Arzt dem Gericht sein Gutachten offenbaren, um seine Interessen wahrzunehmen. Entsprechend darf es der Leistungsträger.

Zu 11.1.3. Ärztlicher/Psychologischer Dienst

Soweit Psychologe und Arbeits- oder Berufsberater bei Teamberatungen des Arbeitslosen zusammenwirken, äußert der Bundesbeauftragte für den Datenschutz Bedenken dagegen, daß Elemente eines psychologischen Gutachtens auch in das zu den Leistungsakten zu nehmende Teamberatungsprotokoll eingehen.

Die Bundesanstalt für Arbeit will dies künftig vermeiden. Gutachterliche Äußerungen des Psychologen sollen künftig nur in sein Gutachten (seinen Bericht, seine Stellungnahme) aufgenommen werden, nicht mehr in das Teamberatungsprotokoll.

Zu 11.2. Krankenversicherung

Zu 11.2.1. Kontrollen

Der Bundesbeauftragte für den Datenschutz regt an, die in den Generalakten der Betriebskrankenkasse des Bundesverkehrsministeriums (BKK) abgelegten

Unterlagen über Personalangelegenheiten von Mitarbeitern der BKK an die personalführende Stelle der Wasser- und Schiffahrtsdirektionen abzugeben.

Der Bundesminister für Verkehr führt hierzu aus, daß die Generalakten der BKK inzwischen von deren Geschäftsführer durchgesehen und diesbezüglich bereinigt worden sind.

Zu 11.2.2. Einzelfragen

— Der Bundesbeauftragte für den Datenschutz regt erneut eine gesetzliche Regelung dahin an, daß der Arbeitgebervertreter in den Selbstverwaltungsorganen der Betriebskrankenkassen nicht der Personalverwaltung des Unternehmens angehören dürfe.

  Hinsichtlich des Geschäftsführers der Betriebskrankenkasse, der wegen der laufenden Führung der Verwaltungsgeschäfte notwendig und ständig Kenntnis von personenbezogenen Daten nehmen muß, vertritt auch der Bundesminister für Arbeit und Sozialordnung die Auffassung, daß der Geschäftsführer einer Betriebskrankenkasse nicht auch in Personalunion in der Personalabteilung des Trägerunternehmens tätig sein darf.

  Hinsichtlich des Vorstandes und der Vertreterversammlung der Betriebskrankenkasse ist die Ausgangslage insofern anders, als Einzelfälle, von sehr seltenen Ausnahmen abgesehen, nicht zu deren kasseninternem Zuständigkeitsbereich gehören, sondern vom Geschäftsführer zu entscheiden sind. Müssen Vorstand oder Vertreterversammlung sich dennoch mit einem Einzelfall befassen, gebietet die Pflicht zur Wahrung des Sozialgeheimnisses, die personenbezogenen Daten zu anonymisieren, bevor sie dem Vorstand oder der Vertreterversammlung der Betriebskrankenkasse vorgelegt werden. Im Rahmen der Strukturreform der Krankenversicherung soll allgemeiner geprüft werden, ob gesetzgeberische Maßnahmen auch zur Verbesserung des Datenschutzes bei Betriebskrankenkassen sinnvoll sind.

— Der Bundesbeauftragte für den Datenschutz vertritt die Auffassung, daß die Krankenkasse einen ihr zulässigerweise übermittelten Entlassungsbericht eines Krankenhauses ohne Einwilligung des Betroffenen nicht dem bei den Landesversicherungsanstalten organisierten vertrauensärztlichen Dienst als Grundlage für die Erstellung eines Gutachtens zur Verfügung stellen dürfe. Die in den §§ 67 bis 77 SGB X genannten Offenbarungsbedingungen, insbesondere des § 76 SGB X, lägen nicht vor.

  Der Bundesminister für Arbeit und Sozialordnung hält diese Auffassung für nicht zutreffend. Die besondere Sperre des § 76 Abs. 1 SGB X gilt nicht für personenbezogene Daten, die im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistungen stehen (§ 76 Abs. 2 SGB X). Eine solche Begutachtung ist auch der der Krankenkasse übersandte Entlassungsbericht des Krankenhauses. Zwar wird der ärztliche Entlassungsbericht nicht zur Erlangung der Sozialleistung erstellt. Gesetzgeberischer Grund für § 76 SGB X war, daß die besonders sensitiven Krankheitsdaten, soweit sie aus Abrechnungsgründen an die Kasse gelangen und deshalb hinsichtlich medizinischer Details weniger zuverlässig sein könnten, im Prinzip nicht von Leistungsträger zu Leistungsträger weiter übermittelt werden sollen.

  Dagegen sollen Aussagen, bei denen es — wie beim Entlassungsbericht des Krankenhauses — auch für weitere Behandlungsentscheidungen auf medizinische Zuverlässigkeit ankommt, bei allen Leistungsträgern verwertbar sein (vgl. Maier, Die Sozialgerichtsbarkeit 1983 S. 89, 93; BfA-Kommentar zu § 76 SGB X, Anm. 4.4).

  Daneben dürfte es Fälle geben, in denen von einem Arzt der Kasse außerhalb eines Gutachtens übermittelte Daten vom vertrauensärztlichen Dienst zur Erfüllung seiner Aufgaben benötigt werden. Es ist dann im Einzelfall zu prüfen, ob die Übermittlung im Rahmen der in § 76 Abs. 1 SGB X gemeinten Rechtfertigungsgründe, die gewohnheitsrechtlich dem Arzt zur Seite stehen, gerechtfertigt wäre. Zu denken ist primär an die Wahrnehmung berechtigter Interessen.

— Der Bundesbeauftragte für den Datenschutz behandelt einen bekanntgewordenen Einzelfall: Ein Leiharbeitsunternehmen verlangte von Arbeitnehmern die Einwilligung, daß die gesetzliche Krankenkasse dem Arbeitgeber eine Bescheinigung über die Krankheitszeiten des Arbeitnehmers in den letzten 12 Monaten erteile.

  Der Bundesminister für Arbeit und Sozialordnung teilt die Auffassung des Bundesbeauftragten für den Datenschutz, daß das Einholen von Auskünften bei den Krankenkassen nicht zu einer Umgehung der arbeitsrechtlichen Rechtsprechung zum Fragerecht des Arbeitgebers und des Schutzes der Sozialdaten führen darf.

  Eine gesonderte gesetzliche Regelung des bisher singulären Sachverhalts wird vom Bundesminister für Arbeit und Sozialordnung für nicht erforderlich gehalten. In der Praxis wird die erbetene schriftliche Auskunft statt dem Arbeitgeber nur dem Arbeitnehmer erteilt. Würde es um sich greifen, daß der Arbeitgeber die Aushändigung der Auskunft an sich durchsetzt, wird man möglicherweise auch die Erteilung der Auskunft an den Arbeitnehmer einschränken müssen.

  Dies wird im Einvernehmen zwischen Versicherungsaufsicht und Krankenkassen zu erreichen sein.

— Der Bundesbeauftragte für den Datenschutz hält verschiedene Maßnahmen der Krankenkassen bei der Mitgliederwerbung für unzulässig.

  Der Bundesminister für Arbeit und Sozialordnung führt hierzu aus:

  a) Soweit Krankenkassen die ihnen als Einzugsstellen für Rentenversicherungsbeiträge bekanntwerdenden Adressen von Nichtmitgliedern zu Werbezwecken verwenden, ist dies

kein Datenschutzproblem, weil die bereichsspezifische Regelung des § 69 Abs. 1 Nr. 1 SGB X die Verwendung von Daten aus dem Bereich der sozialen Sicherung für andere Aufgaben dieses Bereichs auch im Verhältnis mehrerer Träger untereinander zuläßt. Die Nutzung solcher Daten stellt vielmehr ein Problem fairen Wettbewerbs unter Trägern öffentlicher Verwaltung dar.

b) Soweit Krankenkassen Arbeitgeber auffordern, Anschriften von Berufsanfängern und neu einzustellenden Mitarbeitern zu Werbezwecken mitzuteilen, verstößt der Arbeitgeber gegen die ihm obliegende Pflicht zur Verschwiegenheit, wenn er die Mitteilung ohne Einwilligung des Einzustellenden vornimmt.

   Die Krankenkasse darf Adressenmaterial für Aufklärung und Werbung nicht verwenden, wenn die Möglichkeit besteht, daß es unter Verstoß gegen Datenschutzbestimmungen erlangt oder weitergegeben wurde. Die Krankenkasse hat sich deshalb vor der Verwendung von Adreßmaterial des Arbeitgebers für Werbezwecke versichern zu lassen, daß die Einwilligung des Betroffenen eingeholt wurde.

c) Soweit der Arbeitgeber dem Arbeitnehmer in dienstlicher Funktion (z. B. als in der Datenverarbeitung Tätigem oder durch ein betriebsinternes Mitteilungsblatt) die Namen oder Anschriften von Arbeitskollegen zugänglich macht, dürfte die Weitergabe dieser Daten zu Werbezwecken den gleichen Schranken wie oben zu b) unterliegen.

d) Soweit Kenntnisse über Anschriften nicht auf einer Mitteilung beruhen, die Verschwiegenheitspflichten in bezug auf die mitgeteilten Tatsachen auslöst (Beispiel: Kenntnis über Anschriften aus dem sozialen Kontakt unter Mitschülern oder Arbeitskollegen), liegt in der Mitteilung an die Krankenkasse zu Werbezwecken ohne Einwilligung des Betroffenen nichts Rechtswidriges. Entsprechend kann auch die Nutzung dieser Daten durch die Krankenkasse zu Werbezwecken nicht rechtswidrig sein.

Zu 12. Öffentliche Sicherheit

Zu 12.1. Probleme und Hindernisse

Nach den Ausführungen des Bundesbeauftragten für den Datenschutz ergeben sich bei der Erfüllung seiner Aufgaben im Sicherheitsbereich Schwierigkeiten, weil die unter Berücksichtigung des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 erforderlichen Gesetze mit Vorgaben für die Verarbeitung personenbezogener Daten in diesem Bereich, abgesehen von dem Gesetz über das Zentrale Verkehrsinformationssystem beim Kraftfahrt-Bundesamt (ZEVIS), noch nicht verabschiedet worden sind.

Die Bundesregierung beabsichtigt, die in der vergangenen Legislaturperiode begonnenen Arbeiten zur Schaffung der notwendigen bereichsspezifischen Regelungen für die informationelle Zusammenarbeit der Sicherheitsbehörden fortzusetzen und die Entwürfe

— eines neuen Verfassungsschutzgesetzes
— eines Gesetzes über den Militärischen Abschirmdienst
— eines Verfassungsschutzmitteilungsgesetzes
— eines neuen BKA-Gesetzes und
— eines neuen BGS-Gesetzes

im Jahre 1988 im Deutschen Bundestag einzubringen. Unabhängig davon wird der Bundesbeauftragte für den Datenschutz jedoch bereits jetzt bei neuen Verfahren zur Verarbeitung personenbezogener Daten im Sicherheitsbereich beteiligt, und datenschutzrechtliche Aspekte werden soweit als möglich berücksichtigt.

Zu dem Verzicht auf Ausführungen über das Bundesamt für Verfassungsschutz im Neunten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, der angeblich auf überzogene Bedenken des Bundesministeriums des Innern und des Bundesamtes für Verfassungsschutz wegen des Verstoßes gegen Geheimhaltungsvorschriften zurückzuführen ist, wird unter Nummer 14 Stellung genommen.

Zu 12.2. Gesetzgebungsvorhaben

Wie bereits unter Nummer 12.1 ausgeführt, beabsichtigt die Bundesregierung, die nach dem Volkszählungsurteil des Bundesverfassungsgerichts erforderlichen Gesetzentwürfe zur Regelung der informationellen Zusammenarbeit der Sicherheitsbehörden im Jahr 1988 im Deutschen Bundestag einzubringen. Die im Rahmen von Anhörungen zu den in der 10. Legislaturperiode eingebrachten Gesetzentwürfen dargelegte Auffassung des Bundesbeauftragten für den Datenschutz soll in die Überlegungen einbezogen werden.

Zu 12.3. Neufassung der Sicherheitsüberprüfungsrichtlinien

Die Bundesregierung beabsichtigt, noch in der laufenden Legislaturperiode den Entwurf eines Geheimschutzgesetzes zu erarbeiten.

Der vom Bundesbeauftragten für den Datenschutz erwähnte Entwurf neuer Sicherheitsüberprüfungsrichtlinien befindet sich z. Z. noch in der fachlichen Beratung. Hinsichtlich der vom Bundesbeauftragten für den Datenschutz geforderten Zweckbindung der im Rahmen von Sicherheitsüberprüfungen erhobenen Daten muß eine ausgewogene Lösung gefunden werden, die sowohl den Interessen des Betroffenen als auch den Sicherheitsinteressen Rechnung trägt. Die Bundesregierung beabsichtigt, die neuen Sicherheitsüberprüfungsrichtlinien, die auch nach Aussage des an den Arbeiten beteiligten Bundesbeauftragten für den Datenschutz erhebliche datenschutzrechtliche Verbesserungen enthalten, so bald wie möglich zu verabschieden.

Zu 13.1. Datenschutzrechtliche Kontrolle im Bereich der Bekämpfung der Rauschgiftkriminalität

Der Bundesminister des Innern hat im Anschluß an die vom Bundesbeauftragten für den Datenschutz vorgenommene Überprüfung der Datenverarbeitung des BKA im Bereich der Rauschgiftkriminalität zahlreiche datenschutzrechtliche Verbesserungen zugesagt. Der Bundesbeauftragte für den Datenschutz ist der Auffassung, daß diese Verbesserungen noch nicht ausreichend seien. Er befürchtet die Verletzung von Datenschutzbestimmungen und fordert weiterhin Veränderungen in mehreren Bereichen:

— Werden Personendatensätze in Dateien gelöscht, so sind nach Ziffer 8.1 der Dateienrichtlinien grundsätzlich auch die zu den gelöschten Personendatensätzen zugehörigen Unterlagen zu vernichten. Eine derartige Vernichtung ist allerdings aus rein praktischen Gründen dann ausgeschlossen, wenn dieselbe Unterlage nicht nur die Grundlage für Daten bildet, die zu löschen sind, sondern auch die Basis für Daten ist, die noch weiter aufzubewahren sind.

  Das BKA hat deshalb seine Bereitschaft zum Ausdruck gebracht, daß es seine Mitarbeiter für diese Fälle im dienstkundlichen Unterricht ausdrücklich darauf hinweist, daß in Unterlagen aufgefundene Daten nicht mehr verwertet werden dürfen, wenn die dazugehörigen Personendatensätze bereits gelöscht sind.

  Der Bundesbeauftragte für den Datenschutz hält dies jedoch nicht für ausreichend. Er verlangt, daß in den betreffenden Unterlagen alle Daten, die gelöschten Datensätzen zugrunde liegen, durch einen Vermerk eigens gekennzeichnet werden.

  Eine solche Forderung ist mit einem untragbaren Verwaltungsaufwand verbunden und deshalb praxisfremd. Im übrigen hat das BKA seit einiger Zeit seine Mitarbeiter zusätzlich veranlaßt, diejenigen Teile einer Unterlage, die die Grundlage für Daten bildet, die zu löschen sind, durch ein Trennblatt eigens zu kennzeichnen.

— Darüber hinaus verlangt der Bundesbeauftragte für den Datenschutz, daß der Zugriff auf die im Rahmen der Bekämpfung der Rauschgiftkriminalität zentral gespeicherten Daten auf die Dienststellen beschränkt wird, die für die Bekämpfung der Rauschgiftkriminalität zuständig sind.

  Diese Forderung mag auf den ersten Blick plausibel erscheinen, geht aber an der Realität im Bereich der Rauschgiftbekämpfung vorbei. Bereits in der Stellungnahme des Bundesministers des Innern vom November 1985 zum Bericht des Bundesbeauftragten für den Datenschutz über seine Kontrolle der Datenverarbeitung im Bereich der Rauschgiftkriminalität wurde ausdrücklich darauf hingewiesen, daß die Rauschgiftkriminalität in besonderem Maße mit sog. Begleitkriminalität, und zwar insbesondere Beschaffungskriminalität verbunden ist (z. B. Raub des Rauschgiftsüchtigen, um an Mittel für den Ankauf von Drogen zu kommen; Rezeptfälschung des Rauschgiftsüchtigen). Insofern können für diejenigen Dienststellen, die für die Bekämpfung dieser „Begleitkriminalität" zuständig sind, Informationen aus dem Rauschgiftbereich von großer Bedeutung sein. Damit müssen sie aber auch auf die entsprechenden Daten zugreifen können.

  Die Auffassung des Bundesbeauftragten für den Datenschutz hätte darüber hinaus letztlich zur Konsequenz, daß die bestehende personenbezogene Aktenführung zugunsten einer deliktsbezogenen Aktenführung aufgegeben werden müßte. Damit wäre es aber oftmals nicht mehr möglich, im Bedarfsfall ein kriminalistisch umfassendes zutreffendes Bild der Täterpersönlichkeit zu gewinnen.

— Der Bundesbeauftragte für den Datenschutz hält weiterhin die Verwendung der sog. personengebundenen Hinweise („PHW") für fragwürdig und spricht sich insbesondere für eine Beschränkung der Verwendung von PHW auf Fahndungsdateien und für kurze Überprüfungsfristen aus.

  Die zuständigen Gremien der IMK haben kürzlich beschlossen, drei PHW in Zukunft nicht mehr zu verwenden („geistesschwach", „entmündigt", „internationaler Rechtsbrecher") und der Frage der Kriterien für die Vergabe der PHW, der anwendungsbezogenen Speicherung sowie der Speicherfristen weiter nachzugehen. AK II und IMK werden sich mit der Angelegenheit auf der Basis von Vorschlägen einer auf Anregung des Bundesministers des Innern eingerichteten Ad-hoc-Arbeitsgruppe befassen.

— Nach der Errichtungsanordnung für die Arbeitsdatei PIOS-Rauschgift (APR) können dort die Daten von Beschuldigten, Verdächtigen und „andere Personen" unter bestimmten Voraussetzungen gespeichert werden.

  Aufgrund der von ihm angestellten Überprüfung vermutet der Bundesbeauftragte für den Datenschutz, daß möglichst viele Personen als „Verdächtige" eingestuft werden, damit die strengeren Datenschutzbestimmungen für „andere Personen" umgangen werden. Er hat deshalb vorgeschlagen, für Verdächtige eine kürzere Speicherfrist als für Beschuldigte einzuführen.

  Die Vermutung des Bundesbeauftragten für den Datenschutz ist unbegründet. Der Bundesminister des Innern hat bereits in seiner o. a. Stellungnahme vom November 1985 näher dargelegt, daß die Einstufung als „Verdächtiger" oder als „andere Person" auf Grund einer einzelfallbezogenen Prüfung erfolgt. Ergebnis dieser Prüfung kann sowohl die Einstufung als „Verdächtiger" als auch die Einstufung als „andere Person" sein.

  Für eine weitere Differenzierung bei den Speicherfristen sieht die Bundesregierung deshalb keinen Anlaß.

— Schließlich hält der Bundesbeauftragte für den Datenschutz es für erforderlich, daß bei der Anlage von Kriminalakten im BKA die dazugehörigen Personendatensätze von der zentralen Serviceeinheit nur mit einer kurzen Frist versehen werden. Innerhalb dieser Frist soll dann eine Bestätigung der

Speicherung durch die zuständige Fachdienststelle notwendig werden. Diese müsse dann auch das Aussonderungsprüfdatum — orientiert am Sachverhalt und nicht am Tage der Bearbeitung — endgültig festsetzen.

Der Bundesminister des Innern hat gegenüber dieser Forderung des Bundesbeauftragten für den Datenschutz bereits mehrfach Stellung genommen. Er hat dabei insbesondere darauf verwiesen, daß die Vergabe des Aussonderungsprüfdatums durch die zentrale Serviceeinheit stets von den Fachdienststellen überprüft und ggf. korrigiert wird. Im übrigen ist in der weit überwiegenden Anzahl der Fälle die Anwendung der Regelaufbewahrungsfrist erforderlich und auch verhältnismäßig, so daß es zu einer unterschiedlichen Bewertung durch zentrale Serviceeinheit und Fachdienststelle meist ohnehin nicht kommt.

Der Bundesminister des Innern hat ferner darauf verwiesen, daß in diesem Zusammenhang Nummer 7.5 der Dateienrichtlinien vom BKA beachtet wird. Danach beginnt die Aussonderungsprüffrist grundsätzlich an dem Tag, an dem das Ereignis eingetreten ist, das die Speicherung begründet hat. In der Regel stehen dieses Ereignis und der Tag der Neuanlage der Akte im unmittelbaren zeitlichen Zusammenhang. Besteht ausnahmsweise kein derartiger zeitlicher Zusammenhang, wird das Aktenaussonderungsprüfdatum auch nicht unter Zugrundelegung des Datums der Neuanlage der Akte vergeben.

Die Prüfung, inwieweit im Hinblick auf die Auffassung des Bundesbeauftragten für den Datenschutz in diesem Zusammenhang eine Präzisierung des Bundeskriminalamt-Aktennachweises (BKA-AN) vorgenommen werden muß, konnte noch nicht abgeschlossen werden.

Zu 13.2. Weitere Zunahme der SPUDOK-Anwendungen

Im Zusammenhang mit den Spurendokumentationssystemen (SPUDOK) des BKA wiederholt der Bundesbeauftragte für den Datenschutz im wesentlichen seine Kritik, die er bereits im Siebenten Tätigkeitsbericht (Seiten 66 ff.) und im Achten Tätigkeitsbericht (Seiten 45 ff.) geäußert hat.

Im einzelnen wendet sich der Bundesbeauftragte für den Datenschutz zunächst dagegen, daß durch den angeblich zunehmenden Einsatz von SPUDOK-Verfahren vermehrt auch „andere Personen" gespeichert werden.

„Andere Personen" in diesem Zusammenhang sind Personen, deren personenbezogene Daten nach den Dateienrichtlinien bzw. den einschlägigen Errichtungsanordnungen unter bestimmten Voraussetzungen gespeichert werden dürfen, ohne daß diese Personen bestimmten Personengruppen (insbesondere Beschuldigte und Verdächtige) unterfallen, deren Daten nach den Dateienrichtlinien bzw. Errichtungsanordnungen ohnehin gespeichert werden können.

Die Zahl der SPUDOK-Verfahren ist im wesentlichen davon abhängig, in welchem Umfang das BKA diese Verfahren im Rahmen von Ermittlungsverfahren benötigt. Sie hängt damit zu einem erheblichen Teil von der Zahl der Ermittlungsverfahren und damit von einem Faktor ab, auf den das BKA häufig keinen Einfluß hat.

Die Speicherung dieser „anderen Personen" ist in den Dateienrichtlinien ausdrücklich vorgesehen. Als Ausgleich dafür, daß dadurch personenbezogene Daten von Personen erfaßt werden können, die in der Regel weniger betroffen sind als beispielsweise Verdächtige oder Beschuldigte, sieht Ziffer 4.5 der Dateienrichtlinien vor, daß „andere Personen" über die Tatsache der Speicherung zu unterrichten sind, sobald die Dauer der Speicherung ein Jahr überschritten hat. Diese Unterrichtung kann nach Ziffer 4.5.2 der Dateienrichtlinien zurückgestellt werden, solange durch sie der mit der Speicherung verfolgte Zweck gefährdet würde.

Wenn das BKA die Unterrichtung mit Rücksicht auf den Zweck der Speicherung in diesem Sinn zurückstellt, vernachlässigt es deshalb nicht — wie der Bundesbeauftragte für den Datenschutz behauptet — „kontinuierlich die besonderen Schutzvorkehrungen" für „andere Personen", sondern wendet lediglich die — im Zusammenwirken mit dem Bundesbeauftragten für den Datenschutz erstellten — Dateienrichtlinien an.

Im übrigen hat die Bundesregierung bereits in ihrer Stellungnahme zum Achten Tätigkeitsbericht ausdrücklich darauf hingewiesen, daß SPUDOK-Dateien in der Regel nach Abschluß der Ermittlungen gelöscht werden. Dadurch wird auch die Erfassung „anderer Personen" beseitigt.

Da von einer ständigen Zunahme von SPUDOK-Dateien nicht gesprochen werden kann, ist auch die weitere Befürchtung des Bundesbeauftragten für den Datenschutz gegenstandslos, daß es zu einer weiteren Erfassung von Anzeigeerstattern, Hinweisgebern und Zeugen kommt, die nach Ziffer 4.2.10 der Dateienrichtlinien nur in SPUDOK-Dateien gespeichert werden dürfen. Ferner bemängelt der Bundesbeauftragte für den Datenschutz die Qualität einzelner SPUDOK-Errichtungsanordnungen. Diese bestünden insbesondere gelegentlich nur aus vorgefertigten Texten, in die lediglich Aktenzeichen und einige wenige Besonderheiten des einzelnen SPUDOK-Verfahrens eingetragen werden.

Es trifft zu, daß bei der Erstellung einzelner Errichtungsanordnungen der Notwendigkeit Rechnung getragen werden mußte, SPUDOK-Dateien mitunter sehr kurzfristig errichten zu müssen.

Das BKA wird verstärkt dafür Sorge tragen, darin begründete Unzulänglichkeiten bei den Errichtungsanordnungen für SPUDOK-Verfahren abzustellen.

Bei der SPUDOK-Datei „FREDI 86" ging es darum, die Fahndung nach einem ausgebrochenen Häftling zu erleichtern. Mit Rücksicht auf die Gefährlichkeit des Entwichenen — der Betreffende war wegen Mordes, versuchten Mordes, räuberischer Erpressung in vier Fällen, versuchter räuberischer Erpressung und

Raubes zu lebenslanger Freiheitsstrafe verurteilt — mußte die Errichtungsanordnung für die Datei „FREDI 86" sehr schnell erstellt werden. In der Passage der Errichtungsanordnung, die sich mit dem Personenkreis befaßt, der in der Datei Aufnahme finden kann, ist ausdrücklich auf das zugrundeliegende Verfahren der zuständigen Staatsanwaltschaft Bezug genommen worden. Damit war — jedenfalls für die mit der Datei befaßten Mitarbeiter — der erfaßbare Personenkreis hinreichend bestimmt. Es ist deshalb abwegig, wenn der Bundesbeauftragte für den Datenschutz behauptet, in der Datei hätten die Daten „beliebig vieler Bürger" gespeichert werden können, „sofern sie irgendwann einmal irgendeine Straftat begangen haben oder Mitglieder oder Unterstützer irgendeiner Gruppe sind".

Die SPUDOK-Datei „FREDI 86" ist unmittelbar nach der Festnahme des Gesuchten (Frühjahr 1987) gelöscht worden.

Auch in der Errichtungsanordnung für die SPUDOK-Datei „BILLET" ist in der Passage, die sich mit dem Personenkreis befaßt, der in der Datei Aufnahme finden kann, auf das Ermittlungsverfahren der zuständigen Staatsanwaltschaft verwiesen worden. Damit war — jedenfalls für die beteiligten Mitarbeiter — auch hier hinreichend klar, wer zu diesen Personen gehört. Dies gilt im Gegensatz zu der Auffassung des Bundesbeauftragten für den Datenschutz auch für Verdächtige, bei denen zu vermuten ist, daß sie Mitglieder oder Unterstützer einer Gruppe im Zusammenhang mit dem — in der Errichtungsanordnung ausdrücklich bezeichneten — Ermittlungsverfahren sind.

Zu 13.3. Inbetriebnahme der Datei APIS

Der Bundesbeauftragte für den Datenschutz sieht unter mehreren Aspekten bei der am 2. Januar 1986 in Betrieb genommenen „Arbeitsdatei PIOS-Innere Sicherheit" (APIS) datenschutzrechtliche Probleme. Zu den einzelnen Kritikpunkten ist folgendes zu bemerken:

— Der Bundesbeauftragte für den Datenschutz nimmt zunächst Anstoß daran, daß auch sog. Kleinkriminalität in APIS erfaßt wird.

  Aus der Wiedergabe des Wortlauts der einschlägigen Passage der Errichtungsanordnung durch den Bundesbeauftragten für den Datenschutz entsteht der Eindruck, daß der Bundesbeauftragte für den Datenschutz insoweit von einer Fassung der Errichtungsanordnung (6. Januar 1986) ausgeht, die nicht mehr aktuell ist. Dies ist insofern schwer verständlich, als der Bundesbeauftragte für den Datenschutz in einer ausführlichen Stellungnahme vom 25. März 1986 über Wortlaut und Entstehungsgeschichte der diesbezüglichen Neufassung der Errichtungsanordnung informiert worden ist. Mit Schreiben vom 6. Juni 1987 wurde der Bundesbeauftragte für den Datenschutz nochmals auf die Neufassung aufmerksam gemacht, als ihm der Wortlaut der vollständigen Errichtungsanordnung (mit Stand vom 17. April 1986) zugeleitet worden ist.

  Nach der gegenwärtig aktuellen Errichtungsanordnung (Stand 17. April 1986) können Erkenntnisse von anderen Straftaten als den in Nummern 2.1.1 bis 2.1.9 der Errichtungsanordnung ausdrücklich benannten Staatsschutzdelikten nur dann in APIS gespeichert werden, wenn mit diesen Straftaten i. S. der Nummer 1 der Richtlinien für den Kriminalpolizeilichen Meldedienst in Staatsschutzsachen (KPMD-S) verfolgt werden. Dadurch ist sichergestellt, daß strafrechtlich relevante Verstöße gegen die Rechtsordnung mit einer „politischen Motivation" nur dann zu einer Speicherung in APIS führen, wenn die „politische Motivation" sich nicht gegen irgendwelche politischen oder rechtlichen Gegebenheiten, sondern gegen die Verfassungsordnung richtet. Eine solche Motivation kann nach einhelliger Auffassung von Bund und Ländern gelegentlich auch im Rahmen sog. Kleinkriminalität zum Ausdruck kommen.

  Auf diese Gesichtspunkte ist der Bundesbeauftragte für den Datenschutz ebenfalls in der o. a. Stellungnahme vom 25. März 1986 hingewiesen worden. Aus der diesbezüglichen Passage im Neunten Tätigkeitsbericht wird nicht erkennbar, ob der Bundesbeauftragte für den Datenschutz sich mit diesen Argumenten auseinandergesetzt hat.

— Weiterhin hält es der Bundesbeauftragte für den Datenschutz für problematisch, daß in APIS die Datei PIOS-Terrorismus mit den Datensammlungen des polizeilichen Staatsschutzes zusammengeführt wird, damit würden schwere terroristische Straftaten und allgemeine Kriminalität bis hin zur Kleinkriminalität „in einen Topf geworfen".

  Der Bundesbeauftragte für den Datenschutz ist mit dem o. a. Schreiben vom 25. März 1986 auf die Gründe hingewiesen worden, die eine Zusammenlegung beider Datenbestände erforderlich machen. Dazu gehört beispielsweise die gesicherte Erkenntnis, daß Linksextremisten teilweise auch dem linksterroristischen Umfeld zuzurechnen sind und Rechtsextremismus und Rechtsterrorismus untrennbar miteinander verbunden sind. Im übrigen ist es nicht sachgerecht, im Rahmen von APIS zwischen den Datenbeständen aus dem Terrorismus-Bereich und aus dem polizeilichen Staatsschutz einen Gegensatz in der Weise konstruieren zu wollen, daß Straftaten aus dem Terrorismus-Bereich notwendigerweise ungleich schwerwiegender und deshalb mit Straftaten aus dem Staatsschutzbereich nicht vergleichbar seien. Gerade die in der Errichtungsanordnung vorgenommene Beschränkung im Staatsschutzbereich aus Straftaten, bei denen sich die politische Motivation gegen die Verfassungsordnung richtet, engt die Erfassung auf wenige, dafür aber schwerwiegende Rechtsverstöße ein.

— Im Hinblick auf diesen Zusammenhang der in APIS einzustellenden Erkenntnisse wird von der Bundesregierung die Gefahr einer „Verwischung von Datenverarbeitungsmaßstäben", auf die der Bundesbeauftragte für den Datenschutz hinweist, nicht gesehen. Dies gilt auch für die personenbeschreibenden Daten der sog. L-Gruppe. Daß mit Hilfe dieser Merkmale, wie der Bundesbeauftragte

für den Datenschutz vermutet, Körper- und Verhaltensbeschreibungen mit „mehreren hundert Einzelinformationen" zusammengefügt werden, ist praktisch nicht vorstellbar. Gemäß Nummer 5.3.2 der Errichtungsanordnung für APIS stehen für eine Personenbeschreibung lediglich 12 Datenfelder zur Verfügung, die vielfach nur mit je einem Begriff belegt werden (z. B. das Datenfeld „Geschlecht" mit männlich oder weiblich).

— Im Gegensatz zu der Behauptung des Bundesbeauftragten für den Datenschutz wurden auch vor Inbetriebnahme der Datei APIS Daten „anderer Personen" im Bereich des polizeilichen Staatsschutzes gespeichert. Insbesondere mit der Speicherung dieses Personenkreises hing die vom Bundesbeauftragten für den Datenschutz in seinem Sechsten Tätigkeitsbericht (Seite 46) ausdrücklich hervorgehobene Bereinigung von Aktenbeständen des BKA zusammen.

  Im übrigen sieht die Errichtungsanordnung für APIS für die Speicherung von „anderen Personen" (andere als Beschuldigte, Verdächtige, Gefährdete und Geschädigte) besonders kurze Speicherfristen vor (längstens 2 bzw. 3 Jahre).

— Der Bundesbeauftragte für den Datenschutz hält es unter Hinweis auf das föderative Prinzip ferner für bedenklich, daß jeder Teilnehmer an APIS befugt ist, an von anderen Teilnehmern eingestellten Datensätzen unmittelbar Veränderungen oder Ergänzungen vorzunehmen.

  Hierzu ist zunächst zu bemerken, daß eine derartige Befugnis keine Besonderheit von APIS ist, sie ist allen Anwendungen auf der Basis von PIOS (neu) gemeinsam. Ferner haben die Länder, deren Interessen nach Auffassung des Bundesbeauftragten für den Datenschutz hier berührt sein sollen, gegen dieses Verfahren keine Bedenken erhoben, sie haben der Errichtungsanordnung für APIS vielmehr ausdrücklich zugestimmt.

— Das Schreiben des Bundesbeauftragten für den Datenschutz vom November 1985 zur angeblichen Pflicht des BKA, sich in den Fällen, in denen es Informationen weitergibt, aktiv nach deren letztem Stand zu erkundigen, ist zum Anlaß für eine eingehende Prüfung genommen worden, die aber noch nicht abgeschlossen werden konnte. Die Bundesregierung bleibt aber bei ihrer bereits in der Stellungnahme zum Achten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz getroffenen Aussage (vgl. Nummer 12.5), daß sie insoweit bemüht ist, den Zielvorstellungen des Bundesbeauftragten für den Datenschutz entgegenzukommen.

— Der Bundesbeauftragte für den Datenschutz kritisiert ferner, daß das BKA weiterhin Fundstellen von Akten aus seiner Abteilung Staatsschutz im nachrichtendienstlichen Informationssystem NADIS einstellt und damit die anderen NADIS-Teilnehmer direkten Zugriff auf diese Fundstelle haben. In diesem Zusammenhang behauptet der Bundesbeauftragte für den Datenschutz, ursprünglich sei geplant gewesen, mit der Einführung von APIS die Speicherung von BKA-Fundstellen im NADIS entfallen zu lassen, weil sie dann nicht mehr erforderlich sei.

Diese Behauptung ist eine verkürzte und unzutreffende Wiedergabe dessen, was der Bundesminister des Innern in seinem Schreiben vom 25. März 1986 an den Bundesbeauftragten für den Datenschutz ausgeführt hat. In dieser Stellungnahme ist ausdrücklich darauf hingewiesen worden, daß ein Rückzug des BKA aus NADIS nach der Einführung von APIS die Klärung der Frage voraussetzt, auf welche sonstige Weise das berechtigte Informationsinteresse des Verfassungsschutzes in bezug auf polizeiliche Staatsschutzerkenntnisse sichergestellt werden kann; diese Frage ist im Zusammenhang mit der Novellierung des Bundesverfassungsschutzgesetzes und der Schaffung eines Verfassungsschutzmitteilungsgesetzes zu sehen.

Insofern muß der weitere Gang des Gesetzgebungsverfahrens zunächst abgewartet werden.

Zu den weiteren Aspekten, die den Bundesbeauftragten für den Datenschutz veranlaßt haben, diese gegenwärtige Praxis zu beanstanden, ist folgendes zu bemerken:

○ Von der Abteilung Staatsschutz des BKA werden nur solche Personalien von Beschuldigten oder Verdächtigen mit der jeweiligen Aktenfundstelle in NADIS eingestellt, die auch in APIS — bzw. bei nachrichtendienstlichem Hintergrund in der Arbeitsdatei „PIOS-Landesverrat" (APLV) — erfaßt werden. Nach den bereits erwähnten Präzisierungen der Richtlinien für den kriminalpolizeilichen Meldedienst in Staatsschutzsachen und der Errichtungsanordnung für APIS kann es keinem Zweifel unterliegen, daß die dem BKA zugehenden Meldungen, die zu einer Speicherung in der Datei APIS oder der Datei APLV führen, auch von Relevanz für die Verfassungsschutzbehörden sind. Daß dazu gelegentlich auch die vom Bundesbeauftragten für den Datenschutz so bezeichneten „Bagatellen" gehören können, ist unbedenklich, da diese nur dann in NADIS und APIS (bzw. APLV) erfaßt werden, wenn sich die zugrundeliegende politische Motivation gegen die Verfassungsordnung richtet und damit eine verfassungsschutzmäßige Relevanz gegeben ist. Im übrigen ist zu berücksichtigen, daß durch die Speicherung in NADIS die NADIS-Teilnehmer aufgrund der Struktur von NADIS lediglich in Erfahrung bringen können, ob zu einer bestimmten Person relevante Informationen beim BKA vorliegen. Die Übermittlung einzelner Erkenntnisse ist dagegen ausschließlich durch konventionelle Anfragen möglich.

  Schließlich erfolgt eine auf den Einzelfall bezogene Relevanzprüfung durch das BKA als übermittelnde Stelle und die jeweilige Verfassungsschutzbehörde als Empfänger stets dann, wenn aufgrund einer durch NADIS-Abfrage festgestellten BKA-Fundstelle der zugrundeliegende Sachverhalt konventionell mitgeteilt wird.

○ Der Zugriff von Bundesnachrichtendienst und Militärischem Abschirmdienst auf die in NADIS

gespeicherten Fundstellen des BKA erfolgt nur im Rahmen von Sicherheitsüberprüfungen. Der dafür vorgesehene und vom Bundesbeauftragten für den Datenschutz kritisierte Bandabgleich dient der Arbeitserleichterung. Würde er eingestellt, müßten die genannten Behörden konventionell anfragen.

Rechtsgrundlage für diese — gegenständlich sehr begrenzte — informationelle Zusammenarbeit sind jedenfalls bis zum Inkrafttreten eines novellierten Bundesverfassungsschutzgesetzes, eines MAD-Gesetzes und eines diese Zusammenarbeit regelnden Gesetzes §§ 1, 3 Abs. 4 Bundesverfassungsschutzgesetz i. V. m. § 10 Abs. 1 BDSG und den die Aufgaben des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes festlegenden Dienstanweisungen.

○ Falls die Informationen des BKA im Staatsschutzbereich im Einzelfall unvollständig sein sollten oder die Gefahr der Unvollständigkeit besteht, wird dies bei der Beantwortung der konventionellen Anfragen des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes mitgeteilt. Insofern wirkt sich eine Speicherung von Personendaten in NADIS-PZD, bei denen der zugrundeliegende Sachverhalt beim BKA nicht vollständig bekannt ist, im Gegensatz zur Auffassung des Bundesbeauftragten für den Datenschutz nicht nachteilig aus.

Zu 14. Bundesamt für Verfassungsschutz (BfV)

Nach der Darstellung des Bundesbeauftragten für den Datenschutz sind die Ausführungen über das BfV aus dem Neunten Tätigkeitsbericht ausgeklammert und dem Innenausschuß des Deutschen Bundestages als Verschlußsache zugeleitet worden, weil er aus Geheimhaltungsgründen keine andere Möglichkeit gesehen habe.

Dem Bundesbeauftragten für den Datenschutz ist mit Schreiben des Bundesministers des Innern vom 30. Dezember 1986 mitgeteilt worden, welche Passagen seines Berichtsentwurfs vertraulich zu behandeln sind. In den vergangenen Jahren wurden inhaltsgleiche Bitten vom Bundesbeauftragten für den Datenschutz überwiegend akzeptiert und VS-geschützte Teile der Tätigkeitsberichte so umformuliert, daß die vorgetragenen Bedenken entfielen. Beim Neunten Tätigkeitsbericht, der vor allem die datenschutzrechtlichen Fortschritte beim BfV schilderte, wurde dagegen vom Bundesbeauftragten für den Datenschutz ohne den Versuch einer Abstimmung mit dem Bundesminister des Innern auf die Ausführungen über das BfV völlig verzichtet.

Der Hinweis auf Geheimhaltungsvorschriften mit dem Ziel, nicht offen verwertbare Aussagen zu streichen oder umzuformulieren, beeinträchtigt auch in keiner Weise das Recht und die Pflicht des Bundesbeauftragten für den Datenschutz, dem Deutschen Bundestag jährlich einen Tätigkeitsbericht zu erstatten, zu dem die Öffentlichkeit Zugang hat (§ 19 Abs. 2 Satz 2 BDSG). Wie frühere Tätigkeitsberichte bewiesen haben, ist die Information der Öffentlichkeit über die Handhabung des Datenschutzes beim BfV auch unter Beachtung der Verschlußsachenanweisung möglich. Das BfV hätte auf Rückfragen des Bundesbeauftragten für den Datenschutz Hinweise für eine mit dem VS-Schutz vereinbarte Darstellung geben können. Sollte ausnahmsweise eine Umformulierung von Passagen, die der Bundesbeauftragte für den Datenschutz zur Erfüllung seiner Berichtspflicht nach § 19 Abs. 2 BDSG für unverzichtbar hält, nicht möglich sein, so könnten diese geheimhaltungsbedürftigen Informationen ergänzend zu dem der Öffentlichkeit zugänglichen Tätigkeitsbericht dem Deutschen Bundestag als Verschlußsache zugeleitet werden.

Zu der Behauptung des Bundesbeauftragten für den Datenschutz, daß mehrere Passagen des Entwurfs seines Tätigkeitsberichts vom Bundesminister des Innern als geheimhaltungsbedürftig bezeichnet worden seien, obwohl sich Aussagen gleichen Inhalts in Veröffentlichungen von Angehörigen des Verfassungsschutzes finden, ist folgendes zu bemerken:

Die Aussage des Bundesbeauftragten für den Datenschutz bezieht sich auf den Kommentar Borgs/Ebert „Das Recht der Geheimdienste". Dieser Kommentar setzt sich in erster Linie abstrakt mit Rechtsfragen auseinander. In welcher Weise sich die aus dem Bundesverfassungsschutzgesetz und anderen einschlägigen Vorschriften abgeleitete Rechtslage in der Verfahrensweise und den Dienstvorschriften des BfV niederschlägt, wird dagegen nicht beschrieben. Die vom BfV geübte Praxis wird nur dargestellt, wenn sie inhaltlich vorher allgemein bekannt war (z. B. Frage der Behandlung von Informationen aus Asylakten) oder bereits frühere Veröffentlichungen (überwiegend des Bundesbeauftragten für den Datenschutz) vorlagen.

In dem Entwurf des Neunten Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz wurden jedoch vertraulich eingestufte Dienstvorschriften und andere interne Handlungsanweisungen des BfV konkret benannt und der Inhalt dieser amtlichen Dokumente — teilweise beinahe wortgleich — wiedergegeben. Die Einwände hinsichtlich der Verletzung von VS-Vorschriften waren wegen des ausdrücklichen Zusammenhangs mit operativen Instrumenten des BfV deshalb auch dann zu erheben, wenn einzelne materielle Informationen für sich gesehen nicht besonders schutzbedürftig waren. Vielfach hätten die geäußerten Bedenken deshalb durch Umformulierung ohne Schwierigkeiten ausgeräumt werden können, und ein Verzicht auf die Veröffentlichung im Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz wäre nicht erforderlich gewesen.

Zu 16. Bundesgrenzschutz

Zu 16.1. Grenzaktennachweis (GAN)

Der Bundesbeauftragte für den Datenschutz bemängelt, daß in der im Berichtsjahr in Kraft gesetzten Errichtungsanordnung für den GAN des Bundes-

grenzschutzes seine datenschutzrechtlichen Bedenken weitgehend unberücksichtigt geblieben sind.

So beanstandet der Bundesbeauftragte für den Datenschutz, daß Amtshilfeersuchen der Nachrichtendienste als ausreichende Grundlage für die Anlegung von Grenzakten und zur Speicherung im GAN angesehen werden.

Der Bundesminister des Innern stellt hierzu fest, daß Amtshilfeersuchen der Nachrichtendienste bis zur spezialgesetzlichen Regelung in Vollziehung des Volkszählungsurteils übergangsweise auf der Grundlage der bestehenden Gesetze nach der Dienstanweisung zur Durchführung der Amtshilfeersuchen der Verfassungsschutzbehörden und des BND in der Fassung vom 23. Oktober 1981 bearbeitet werden.

Zu den vom Bundesbeauftragten für den Datenschutz geäußerten Bedenken gegen die Verwendung personenbezogener Hinweise bemerkt der Bundesminister des Innern:

Bei den im Sondervermerk in freitextlicher Form eingehenden Schlüsselbegriffen handelt es sich nicht um personenbezogene Hinweise im eigentlichen Sinne, sondern um beispielhaft aufgezählte Merkmale, die dem ermittelnden Beamten ermöglichen sollen, bei seinen Feststellungen diesen Hinweis besonders zu berücksichtigen. Die Beeinträchtigung des Betroffenen wird dadurch merklich gemindert, daß der Beamte nicht die gesamte Palette der Überprüfungsmöglichkeiten zu berücksichtigen hat.

Im übrigen ist die Möglichkeit, spezifisches Täterverhalten freitextlich zu verarbeiten, vom Bundesbeauftragten für den Datenschutz in einem Schreiben vom 12. August 1985 an den Bundesminister des Innern — V 192 642 — 1/21 — selbst angeregt worden.

Die vom Bundesbeauftragten für den Datenschutz vertretene Auffassung, daß es ausreichend sei, wenn der Zugriff auf den GAN über Telefon oder Sprechfunk beim GS-Amt gewährleistet wird, teilt der Bundesminister des Innern nicht.

Der Bundesminister des Innern hält den Direktzugriff auf den GAN nicht nur für die GS-Direktionen und die GS-Ämter, sondern auch für die Geschäftszimmer der GS-Stellen für erforderlich und auch wegen der von den Dienststellen durchzuführenden Aufklärungs- und Ermittlungsmaßnahmen für geboten.

Der Bundesbeauftragte für den Datenschutz bedauert, daß die Relevanzprüfung vor der Übermittlung von Daten und die Pflicht zum Nachbericht entfallen sind.

Der Bundesminister des Innern bemerkt hierzu, daß der GAN eine Ergänzung der KpS-Richtlinien für die besonderen Belange der Grenzpolizei ist. Es ist daher sachgemäß, die in den KpS-Richtlinien enthaltenen Regelungen über die Auskunftserteilung im GAN anzuwenden.

Es muß auch die ergänzende Verantwortung der Empfänger gesehen werden, erneut anzufragen, ob die ursprünglich übermittelten Daten noch aktuell sind, wenn er diese Informationen verwerten will (vgl. auch Stellungnahme der Bundesregierung zum Sechsten Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, Seiten 33 ff.).

Zu 16.2. Restriktive Datenschutzpraxis beim Grenzschutzkommando Nord

Der Bitte des Bundesbeauftragten für den Datenschutz, die Liste der Demonstrationsteilnehmer aus dem Sachvorgang zu entfernen, ist entsprochen worden.

Zu 18. Verteidigung

Zu 18.1. Fehlende Rechtsgrundlage für die Datenverarbeitung beim MAD

Der Bundesbeauftragte für den Datenschutz hält die Verarbeitung personenbezogener Daten beim MAD ohne ausreichende Rechtsgrundlage nur noch für einen begrenzten Zeitraum für hinnehmbar. Für problematisch hält der Bundesbeauftragte für den Datenschutz, Rechtseingriffe durch den MAD auf die Grundsätze des sog. „Übergangsbonus" zu stützen.

Die Bundesregierung hat ihren wiederholt zum Ausdruck gebrachten Willen, die Aufgabenwahrnehmung des MAD gesetzlich zu regeln, in der vergangenen Wahlperiode durch Einbringung des Entwurfs eines Gesetzes für den Militärischen Abschirmdienst (Drucksache 10/5342) bekräftigt. Da der Gesetzentwurf aus Zeitgründen nicht mehr verabschiedet werden konnte, ist beabsichtigt, ihn in der 11. Wahlperiode erneut den Gesetzgebungskörperschaften zuzuleiten. Bis zur Verabschiedung des Gesetzes soll den vom Bundesverfassungsgericht zum „Übergangsbonus" aufgestellten Rechtsgrundsätzen (insbesondere in BVerfGE Bd. 41 S. 266 ff. und Bd. 51 S. 287 ff.) dadurch Rechnung getragen werden, daß Aufgaben und Befugnisse des MAD unter Einhaltung der Grenzen, die durch die Bestimmungen des genannten Gesetzentwurfs gezogen wurden, in einer Dienstvorschrift alsbald neu bestimmt und eingegrenzt werden.

Zu 18.2. Neukonzeption für die Merkmalspeicherung beim MAD

Der Bundesbeauftragte für den Datenschutz beanstandet, daß dem MAD künftig wieder gestattet werden soll, einige wenige Daten aus der engeren Persönlichkeitssphäre, die bei der Sicherheitsüberprüfung von Angehörigen des Geschäftsbereichs des Bundesministers der Verteidigung gewonnen werden, zu speichern.

Die Bundesregierung hält die Kritik des Bundesbeauftragten für den Datenschutz für unbegründet. Sie bemerkt hierzu, daß ähnliche Speicherungen zwar nach einer Beanstandung des Bundesbeauftragten für den Datenschutz im Jahre 1983 eingestellt bzw. gelöscht wurden. Dies führte in der Folgezeit jedoch zu einer Beeinträchtigung der Aufgabenwahrnehmung im MAD. Im Hinblick darauf ist im Jahre 1986 erwogen worden, die Speicherung bestimmter persönlicher

Daten aus der engeren Persönlichkeitssphäre wieder zuzulassen. Hierbei konnte den datenschutzrechtlichen Bedenken des Bundesbeauftragten für den Datenschutz jedoch weitgehend Rechnung getragen werden. So wurde der Katalog der zu speichernden Daten gegenüber dem Stand von 1982 erheblich reduziert. Auch wurden die Voraussetzungen für eine Speicherung wesentlich verschärft. Darüber hinaus soll nur ein engbegrenzter Personenkreis Zugriff auf die gespeicherten Daten haben. Schließlich ist beabsichtigt, die gespeicherten Persönlichkeitsdaten nur für Zwecke der Sicherheitsüberprüfung und der Spionageabwehr zu nutzen. Bis zur Einrichtung des geplanten Zugriffsschutzes findet die Speicherung von Daten aus dem engeren Persönlichkeitsbereich nicht statt.

Die Gespräche des Bundesministers der Verteidigung mit dem Bundesbeauftragten für den Datenschutz zur Neukonzeption für die Merkmalspeicherung beim MAD sind im übrigen noch nicht abgeschlossen.

Zu 23. Bilanz

Die Auffassung des Bundesbeauftragten für den Datenschutz, daß eine gesetzliche Regelung für das Schuldnerverzeichnis erforderlich sei, wird von der Bundesregierung geteilt. Ein entsprechender Gesetzentwurf wird vom Bundesminister der Justiz vorbereitet.

Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 13 63, Herderstraße 56, 5300 Bonn 2, Telefon 02 28/36 35 51, Telefax 02 28/36 12 75
ISSN 0722-8333